IBAT College Dublin Associated Policies and Standard Operating Procedures 2023/24 – Version 4.11 March 20th 2025

Update approved by Academic Council on 20.03.2025

Contents

1. Policies

AP 1.1 IBAT College Dublin Risk Management Policy

IBAT College Dublin

November 2017

1.0 Background

This risk management policy (the policy) forms part of the College's internal controls and corporate governance arrangements. Effective risk management is an essential element in the framework of good corporate governance in higher education institutions (HEIs). The Statutory Quality Assurance Guidelines developed by Quality and Qualifications Ireland (QQI) for use by all Providers (April 2016) has specified that a system of governance should be in place that considers risk and that the system of governance has procedures in place to ensure that the provider is not engaged in activities or partnerships that might undermine the integrity of the education and training offered or the awards in the National Framework of Qualifications to which they lead, either in Ireland or abroad. Risk extends to the mode of provision, for example, alternative modes of delivery not embraced by the QA system. The consideration of risk also extends to:

- maintaining academic integrity
- the avoidance of academic or other fraud associated with provision and related services
- planning to ensure capacity to provide adequate services to the number and type of students recruited.

2.0 Policy

It is the policy of IBAT College Dublin that risks to the achievement of the strategic objectives and running of the College should be identified, assessed, managed and monitored to support the demonstration of good governance.
The policy explains the College's underlying approach to risk management, documents the roles and responsibilities of the Board of Directors, Board of Governors the Senior Management Group, and other key parties.

3.0 Reference documents

The risk management framework is influenced by the following:

- ISO 3000 family of standards relating to risk
- The Higher Education Funding Council for England publications on risk management
- Risk Management policy of the Institutes of Technology.

4.0 Terminology

4.1 Risk: According to ISO 31000 risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected

Risks, by their very nature, may or may not occur and fall into a variety of categories, some of the most common being:

- **Strategic Risks:** the inability to achieve the College's strategic and operational objectives as set out in the Strategic Plan and, not taking opportunities when they arise;
- **Operational Risks**: the inability to prevent a loss resulting from inadequate internal processes and systems;
- **Financial Risks:** exposure to losses arising because of the need to improve the management of the College's financial assets;
- **Reputational Risks:** exposure to losses arising because of bad press, negative public image and the need to improve stakeholder relationship management.

4.2 **Risk Management** refers to a coordinated set of activities and methods that is used to direct an organisation and to control the many risks that can affect its ability to achieve objectives. It also refers to the architecture that is used to manage risk. This architecture includes risk management principles, a risk management framework, and a risk management process. The approach is shown in **Appendix 1.**

4.3 **Risk assessment** is a process that is, in turn, made up of three processes, risk identification, risk analysis, and risk evaluation

4.3.1 **Risk identification** is a process that is used to find, recognise and describe the risks that could affect the achievement of objectives

4.3.2 **Risk analysis** is a process that is used to understand the nature, sources, and causes, of the risk which has been identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist.

4.3.2 **Risk evaluation** is a process that is used to compare risk analysis results with risk criteria to determine whether or not a specified level of risk is acceptable or tolerable.

4.4 **Risk appetite and tolerance**. Risk appetite can be defined as "the amount of risk and type of risk that an organisation is willing to take in order to meet their strategic objectives" The College can be risk-taking or risk-averse, and different levels of risk appetite can apply to different activities. In deciding its risk appetite, the College will decide the threshold beyond which risks move from being monitored locally, to being monitored by the Board of Governors, or finally to the abandonment of a particular activity. Clarity in relation to the College's risk appetite is critical to enable the Board of Governors to decide on how best to manage any particular risk.

4.4.1 **Risk appetite categories:** Risk elements arising from proposed or actual developments/activities within the College may fall into three categories:

(i) Risks that are trivial and therefore acceptable and do not need to be managed

(ii) Risks that are acceptable and will need to be managed

(iii) Risks that are unacceptable and therefore the development/activity should not proceed.

The concept of risk appetite applies to major developments/activities and is concerned with the placing of a boundary between (ii) and (iii) above. It therefore reflects the College's tolerance of risk.

4.4.2 A major development/activity may be defined as having a value **more than €50,000** or which may pose a significant reputational risk to the College. Any such proposed development/activity and associated risks must be reported to, and authorised by, the Senior Management Group for consideration immediately they arise. This process must be followed also where there is any doubt whether or not a risk associated with any development/activity might be deemed acceptable to the College.

4.5. Management of Risk

Upon completion of a risk assessment and taking account of the College's risk appetite, the College may decide on one of the following:

- treat the risk (e.g. use of internal controls)
- terminate the risk
- tolerate the risk (accept the risk with or without monitoring)
- transfer the risk (e.g. by using insurance, sub-contracting).

5.0 Underlying approach to risk management

The following key principles outline the College's approach to risk management and internal control:

5.1 Board of Directors: Overall responsibility for the management of risk within the College lies with the Board of Directors. The Board of Directors will:

- approve the College's Risk Management Policy
- satisfy itself through its Board of Governors that an adequate Risk Management Framework is in place in the College
- Have oversight of management and corporate issues that affect risk,
- Determine the College's risk appetite and review risk portfolio against appetite.

5.2 Board of Governors: The role of the Board of Governors is to assure the Board of Directors that an adequate Risk Management Framework is in place in the College. In providing the required level of assurance, the Board of Governors will:

- Ensure that Risks are being managed appropriately by the College Senior Management Group
- Keep under review, and advise on, the operation and effectiveness of the College's Risk Management Framework
- Ensure that assurance provided by management and external/internal auditors is appropriate
- Monitor the effectiveness of Risk Management in relation to risks identified as fundamental to the success or failure of the College's strategic objectives

- Report to the Board of Directors on its findings in relation to risk management and the adequacy of the Risk Management Framework on an annual basis.

5.3 Risk Management Function

College Director: The College Director has overall responsibility for ensuring that procedures and processes are in place to enable adherence to this Risk Management Policy. Additionally, the College Director will:

- Ensure the provision of adequate training and awareness to Risk Owners
- Ensure the communication of the key elements of the College's Risk Management Framework
- Maintain the College's Risk Register, including its review and up-date on a twice-annual basis.
- Implementing the College's Risk Management Policy
- Identifying and monitoring risks.

5.4 Senior Management Group

The College's Senior Management Group is responsible for:

- Implementing the College's Risk Management Policy
- Identifying and monitoring Risks
- Ensuring that each risk has a 'Risk Owner' responsible for its management
- Ensuring that controls identified are working, provide periodic positive assurance that they are working and/or report if they are not working
- Ensuring that individuals understand what level of risk they are empowered to take on behalf of the College
- Ensuring local risks are appropriately managed (through consideration of reports on local risk on a twice-annual basis
- Taking particular note of any risks identified locally that should be escalated to the Risk Register
- Reviewing the Risk Register on a twice-annual basis in light of reports on local risk analysis and other relevant matters
- Monitoring the assessment and management of risks that could impact on the achievement of the College's objectives
- Encouraging a risk management culture throughout the College so that risk is embedded as part of the College's decision making and operation
- Critically reviewing the effectiveness of risk management processes
- Report to the Board of Governors through the **Audit Sub-Committee of the Board of Governors** on a twice-annual basis on the College's Risk Register and the implementation of the Risk Management Framework.

5.5 Individual Members of the Senior Management Group

Members of the Senior Management Group are responsible for the following in relation to risk management:

- Implementation of College Policy in relation to Risk Management within their area of control
- The identification, assessment, management and ownership of risk within their area of control
- The establishment and regular review of local risks in their area and its transmission to the Senior Management Group twice-annually or as required
- Members of the Senior Management Group will report twice-annually on local risks within their areas of control
- The identification of new and emerging risks that cannot be managed locally and the reporting of such risks to the Senior Management Group as required but at least twice-annually for escalation to the Risk Register
- Ensuring that all substantial projects or new programmes undergo risk assessment and that such assessment is included in the project/programme proposal, and reporting on same to the Senior Management Group
- Supporting the embedding of risk management in their area and the development of a risk-aware culture.

5.6 Risk Owner

The risk owner oversees the process around the management of a particular risk.

The risk owner's role in relation to risk management includes:

- Coordination of the relevant risk controls
- Ensuring staff are dealing with local risks
- Overall management of the risk.

The owner of each risk is identified in the Risk Register.

5.7 Internal Audit

The Audit Sub-Committee, appointed by the Board of Governors, is responsible for review of internal controls within the College. In developing its Annual Internal Audit Plan cognisance will be taken of the College's Risk Register. The internal audit reviews of College activities/Schools/functions will include a periodic assessment of the effectiveness of their respective risk management processes and will report to the Board of Governors on how those risks are being managed.

6.0 Procedure

6.1 The risks to the successful achievement of the strategic objectives and running of the College shall be identified, assessed, managed and monitored on a predetermined basis:

New risks arising from a new strategic objective shall be identified, assessed, managed and monitored
New risks shall be identified arising from:

- Non-conformances
- Incidents
- Near misses
- Complaints
- Claims

6.2 All risks shall be reassessed on a predetermined basis so that an up to date risk assessment is available to support the management of risk

6.3 Risks shall be assessed using the following approach to ensure consistency of application across the College.
Risks identified must be assessed and measured in accordance with inherent and residual risk criteria as shown in the table below:

	Assessment Inherent	**Residual**
Impact	The extent of impact on the College's operations if the risk arises in the *absence* of mitigating controls.	The extent of impact on the College's operations if the risk arises in the *presence* of mitigating actions and controls.
Likelihood	The probability of the risk arising in the *absence* of mitigating controls.	The probability of the risk arising in the *presence* of mitigating actions and controls.

Table 1. Risk Identification and Assessment

Not all risks are equal and effective risk management is only possible if risks are prioritised appropriately. Generally, risks should be prioritised according to their ability to affect the College achieving its objectives and therefore may change as objectives change.

6.4 The effectiveness of management controls shall be reported, by the relevant risk owners at predetermined intervals to the Senior Management Group and the Audit Sub-Committee:
6.4.1 High level risks every three months
6.4.2 Medium level risks every six months
6.4.3 Low level risks on an annual basis or more frequently if circumstances change

6.5 Senior Management Group shall facilitate audit of the risk management system
6.6 Senior Management Group shall implement corrective and preventive action identified as necessary from monitoring and audit exercises

7.0 Training

Training shall be provided as and when requested to the College Director

8.0 Monitoring and audit

Monitoring and audit shall be undertaken by:

- Senior Management
- Audit Sub-Committee shall undertake audit of the risk management system at pre-determined intervals

9.0 Annual review of effectiveness

9.1 The Board of Governors is responsible for reviewing the effectiveness of risk controls of the College (See section 5.2), based on information provided by the Senior Management Group. Its approach is outlined below. The Audit Sub-Committee on behalf of the Board of Governors will for each significant risk identified, will:

- review the previous year and examine the College's track record on risk management and internal control

- consider the internal and external risk profile of the coming year and consider if current internal control arrangements are likely to be effective

9.2 In making its decision the following will be considered:

9.2.1 control environment;

- the College's objectives and its financial and non-financial targets
- organisational structure
- culture, approach, and resources with respect to the management of risk
- delegation of authority
- public reporting

9.2.2 On-going identification and evaluation of significant risks:

- timely identification and assessment of significant risks
- prioritisation of risks and the allocation of resources to address areas of high risks

9.2.3 Information and communication:

- quality and timeliness of information on significant risks
- time it takes for control breakdowns to be recognised or new risks to be identified

9.2.4 Monitoring and corrective action:

- ability of the College to learn from its problems
- commitment and speed with which corrective actions are implemented

9.3 The Senior Management Group will prepare a report of its review of the effectiveness of the internal control system annually for consideration by the Board of Governors.

10.0 Review of the Policy

This policy will be reviewed every two years to ensure that it continues to enhance the decision-making and operation of the College.

Appendix 1

Guide to Risk Management

1.0 Risk Identification

1.1 The purpose of risk identification is to produce a list of potential risks that could impact on the College achieving its objectives. Risks will be identified under the four headings:

Reputational risks

Financial risks

Strategic risks

Operational risks

Risks will be identified using a variety of techniques such as interviews, meetings, and reference to good practice guidelines.

2.0 Risk Assessment

Having identified a risk, the potential impact and likelihood of the risk being realised will be rated.

The templates are adapted from those used in the Institutes of Technology.

To ensure consistency across the College, the following method will be used in assessing risk (examples supplied) below.

For the purposes of the Risk Assessment Process, the highest ranked rating across the categories will be deemed to be the overall impact assessment, for example, if a reduction in earnings scored a '4' under Financial Impact and '3' under Strategic Impact, then that impact assessment rating would be '4'.

IMPACT RATING		Financial Impact	Examples of Intangible Impacts		
		Financial	Strategic	Operational	Reputational
Extreme	**4**	Over €50,000	Issue with new campus resulting in non - recruitment of students. Significant delay in the development of new programmes. QA policies and procedures not been followed.	Closure/disruption of the College for greater than 2 days Serious debilitating injury/loss of life Cancellation of exams QA policies and procedures not been followed.	Withdrawal of Programme Accreditation by Awarding Body Not maintaining academic integrity
Serious	**3**	€35,000 - €50,000	Significant shortfall in recruitment targets for a number of programmes. Issues with recruiting staff with particular expertise.	Unavailability of IT service of the College for more than 2 days Injury requiring hospitalisation. Postponement of exams	Negative headlines in the national press, radio and television Negative feedback from students on social media
Moderate	**2**	€20,000 - €35,000	Delay in the delivery of a planned new academic programme Shortfall in recruitment targets for a particular programme	Disruption to a few sections of the College and delaying the academic process for up to 1 day. Injury requiring attendance at medical facility Delays in exams	Reputational impact due to negative coverage regarding a staff member or student in local media.
Minor	**1**	Up to €20,000	Minor delay in achievement of a goal	Non-delivery of classes for up to half a day. Injury resulting in cuts/bruises. Disruption to individual exams	Potential damage due to negative coverage of private colleges in the media.

3.0 Likelihood

Analysing risks requires an assessment of their frequency of occurrence also. The following table provides broad descriptions used to support risk likelihood ratings:

Rating Likelihood	
4 Very Probable	Very Likely, will occur in most circumstances (within the next year)
3 Quite Probable	Likely, may occur (once every 1-2 years)
2 Possible	Very Unlikely, may occur at some point (once in 3-5 years)
1 Improbable	Rare, never happen, may occur in exceptional circumstances (once in 5-10 years)

4.0 Risk Rating

When rating the risks identified, use the Heat Map table below to calculate the risk score and then the Classification of Risks below to identify the Risk Rating.

		Likelihood			
		Improbable (1)	Possible (2)	Quite Probable (3)	Very Probable (4)
Impact	Extreme (4)	4	8	12	16
	Serious (3)	**3**	6	9	12
	Moderate (2)	**2**	4	6	8
	Minor (1)	**1**	**2**	**3**	4

Table: Heat Map

Classification of Risks		Score
Extreme	Red	12-16
Serious	Amber	8-11.9
Moderate	Yellow	4-7.9
Minor	Green	1-3.9

5.0 Control Assessment

Assess the strength of control. Where the strength of the control is assessed as highly effective reduce the inherent risk score by 90%. Where the control is assessed as moderate i.e. in place with limited exceptions, reduce the inherent risk score by 60% and where there is no control in place or the control has serious weaknesses, reduce the control by 0%.

6.0 When Risks are Assessed

6.1 The above risk assessment exercise should be carried out at two levels:

- At an 'inherent' risk level where the potential risks affecting the College are assessed in the absence of mitigating actions and controls (at least twice annually)
- At a 'residual' risk level where the risks affecting the College are considered with selected mitigating actions and controls fully implemented (at least twice annually).

6.2 Having identified the inherent risk and the impact and likelihood of that risk, it is necessary to consider the controls which would mitigate the impact and likelihood of that risk being realised. It is essential to distinguish between those controls that are in place and those that are planned. It is then a matter to assess the impact and likelihood of the residual risk being realised. **It is important to note that the assessment of residual risk can only be based on controls already in place.**

6.3 Risk Register

The following template can be used at a local level to capture and analyse risks identified. The example below shows an example of a risk in the financial area and **Residual** Risk Heat Map should be used in the assessment of Risk (the main Risk Register Template is set out in Appendix 2):

Risk No	Risk Description	Risk Category Highlight those that apply		Inherent Risk Rating Impact	Likelihood	Score
REG-001	**Data Breach Occurring** • E-mail sent to numerous people and not bcc or attaching details to a mail. • Inappropriate use of data etc. • Loss of/ compromised or altered data **Data Breach Reporting** • If a breach occurs, and data pertaining to students or staff is compromised / lost or altered inadvertently - staff need to know it happened, how to report / escalate and if the Office of the Data Protection Commissioner needs to be to notified. This will be based on the IBAT DPO determining the materiality of the breach.	Strategic	**X**	4 – Extreme	2 – Minor	8 – Serious
		Reputational	**X**			
		Operational	**X**			
		Financial	**X**			

Current Controls	Control Assessment (Highlight appropriate section)			Control Rating
	H – 90% reduction	M - 60% reduction	L - 0% reduction	**Score**
1. Compilation of data register and assigning frequency of monitoring				

2. Communication with staff on efficacy of having appropriate communications to expressions of interest, students, internally between staff & with lecturers. 3. Review of e-mails by a “second sight” for appropriateness. Conducted currently on an ad-hoc basis.	**Risk Owner** Registrar
Mitigation Strategy	**Action Plan**

6.4 Residual Risk and level of Reporting Required

Residual risk score is the inherent risk rating score multiplied by (1 – Control Assessment Reduction percentage) to give the control rating percentage.

Residual Risk and Level of Report	Residual Risk Score	Further Information
Extreme Board of Directors, Board of Governors	12-16	If the residual risk is deemed to be extreme, then immediate action is required. In this case the activity/project should not proceed or if it relates to an existing activity/project then the Manager of the area, who is a member of the Senior Management Group, must inform the Board of Governors of the matter so that action can be taken immediately to either moderate the risk or close the activity/project.
Serious Board of Governors	**8-11.9**	Serious risks require careful on-going management with frequent evaluation of the risk factors by the manager of the area who is a member of the SMG in order to restore them to more acceptable levels of risk. Risks at this level should be reported to the Board of Governors at its twice-annual risk management meetings. In the interim, any escalation of risk should be reported to the SMT immediately by the relevant SMT member.
Moderate A member of the Senior Management Group	**4-7.9**	Moderate levels of risk may be acceptable for certain projects and these risks require approval of the Head of Function prior to commencing the activity/project or to allow the project/activity to continue. Re-assessment of the risk factors should be conducted at regular intervals to assure stakeholders that the risk has not escalated.

Minor Head of Function	**1-3.9**	This is the lowest and most tolerable level of risk. Student projects and individual staff research should carry no higher than tolerable risk without the express approval of the Head of Function. Re-assessment of the risk factors should be conducted at regular intervals to assure stakeholders that the risk has not escalated.

Appendix 2 Risk Register Template

The following template can be used at a local level to capture and analyse risks identified.

<table>
<tr><th colspan="8">Risk Register Template</th></tr>
<tr><th rowspan="2">Risk No</th><th rowspan="2">Risk Description</th><th rowspan="2" colspan="2">Risk Category
Highlight those that apply</th><th colspan="4">Inherent Risk Rating</th></tr>
<tr><th>Impact</th><th>Likelihood</th><th colspan="2">Score</th></tr>
<tr><td rowspan="4"></td><td rowspan="4"></td><td>Strategic</td><td></td><td rowspan="4"></td><td rowspan="4"></td><td colspan="2" rowspan="4"></td></tr>
<tr><td>Reputational</td><td></td></tr>
<tr><td>Operational</td><td></td></tr>
<tr><td>Financial</td><td></td></tr>
<tr><td colspan="4" rowspan="2">Current Controls</td><td colspan="3">Control Assessment
(Highlight appropriate section)</td><td>Control Rating</td></tr>
<tr><td>H – 90% reduction</td><td>M - 60% reduction</td><td>L - 0% reduction</td><td>Score</td></tr>
<tr><td colspan="4">1.
2.
3.</td><td colspan="3" rowspan="2">Risk Owner</td><td></td></tr>
<tr><td colspan="4"></td><td colspan="2"></td></tr>
<tr><td colspan="3">Mitigation Strategy</td><td colspan="5">Action Plan</td></tr>
<tr><td colspan="3">1.
2.</td><td colspan="5">1.
2.</td></tr>
</table>

AP 1.2 IBAT College Dublin Recognition of Prior Learning (RPL) Policy and Guidelines

Recognition of Prior Learning (RPL)
Policy and Guidelines

2017

IBAT College Dublin, 16-19 Wellington Quay, Temple Bar, Dublin 2

Recognition of Prior Learning (RPL) Policy and Guidelines

1. Introduction

Recognition of Prior Learning (RPL) is a process that allows learners gain admission to a programme of study, advanced entry to a programme of study or to gain exemptions/credit from part of a programme based on demonstrated learning achieved prior to admission.

IBAT College Dublin recognises that learners may have gained relevant knowledge, skills and competencies prior to the commencement of a programme of study. The College, through its RPL policy and practice, recognises appropriate prior learning so that learners do not have to cover topics already mastered, whether this mastery has come through prior study, work or life, or any combination of the three. The College acknowledges that learning can be acquired from a range of learning experiences, including accredited, non-accredited, formal and informal learning. In line with the National Framework of Qualifications (NFQ) the College aims to recognise all learning achievements by facilitating the Recognition of Prior Learning.

Candidates who consider they are eligible for exemption(s) on the basis of prior learning may apply directly to the College. The College will seek to match the learning with the learning outcomes of the subject(s) from which the candidate seeks exemption.

IBAT College Dublin is committed to granting exemptions on admission to its programmes, where/as appropriate. Due to the complexity and nature of the current MBA programme, including the high level of learning attained through the completion of the full programme, the College, at present does not consider applications for exemptions in respect of the MBA. In order to achieve the award of Master of Business Administration, learners must accrue the appropriate number of credits for this programme through participation and assessment.

Assessment of prior experiential learning will be carried out by either the Head of School, Programme Director, or a member of academic staff competent in the subject area and then signed off by the Registrar. The Registrar ensures that the RPL process is applied in a consistent, fair and transparent manner. This process is overseen by the Admissions Committee. Evidence submitted by an applicant is available for review by the External Examiner and the Admissions Committee.

This document provides guidelines designed to ensure consistency and transparency in the application of the Recognition of Prior Learning within the College.

2. Definitions

For the purpose of this document the term RPL is used and incorporates both the Recognition of Prior Certified Learning (RPCL) and the Recognition of Prior Experiential Learning (RPEL).

Recognition of Prior Certified Learning (RPCL): This is where an applicant has already been awarded certification for a formal programme taken at another Institution (in Ireland or abroad). This learning may entitle the applicant entry onto a programme, exemptions from some elements of a programme or advanced entry onto a programme of study.

Recognition of Prior Experiential Learning (RPEL): This involves the awarding of credit for learning gained from experience i.e. learning that has not previously been academically accredited. In this case, the candidate must prove that the required learning outcomes have been achieved. This evidence can then be used to support a claim for admission onto a programme of study, exemption from some elements of a programme or credit. As a general principle, recognition is given for learning and not for experience *per se*.

Formal learning is normally programme-based learning which takes place in a formal setting. It is specifically designated as learning, with specific programme content, learning objectives, stated duration for the programme and learning support.

Non-formal learning is intentional in that it takes place through planned, organised learning activities but typically does not involve certification - for example non-formal learning and training activities undertaken in the workplace.

Informal learning is not organised or structured (in terms of objectives, time or learning support). Informal learning is, in most cases unintentional from the student's perspective. It takes place through life and work experience – and is sometimes referred to as experiential learning. It typically does not lead to certification.

Learning Outcomes: For the purpose of RPL, the learning outcomes refers to a student's knowledge, understanding, skills and/or competences acquired as a result of prior learning.

3. Policy Principles

The following guidelines apply in the implementation of RPL within IBAT College Dublin.

- Through its RPL processes the College recognises learning which has occurred before admission onto a programme or to the relevant stage of a programme of study irrespective of mode or place of learning
- In seeking recognition under RPL, prior learning must be evidenced through a medium that is appropriate to the particular learning outcomes
- The focus of the College's RPL process will be on the achievement of learning, or the outcome of that learning, rather than the experience of learning
- Prior certified learning may entitle the candidate to exemptions on a programme, not credits. Learning which has been previously accredited is not ascribed credit twice
- Exemptions or credits for prior experiential (non-certified) learning may be awarded on the basis of demonstrated learning which shows that a candidate has achieved specified learning outcomes relevant to the programme of study
- Recognition will normally be given for complete modules only and where all of the learning outcomes of a module have been achieved
- The College must ensure that academic standards comparable to those attained on programmes by traditional mode will be maintained and applied throughout the RPL process
- Exemptions are granted where prior learning has not previously been awarded credit under the European Credit Transfer System (ECTS)
- In the case where a candidate presents with a qualification that was achieved outside of Ireland, the qualification will be assessed using the NARIC Ireland Qualifications Recognition database to establish equivalency
- Exemptions / advanced entry can only be granted prior to or/at commencement of a module or stage
- Exemptions are not available on every programme of study available at IBAT College Dublin. Where such an exception occurs, clear information with be provided via the programme documentation available to applicants and learners and on the College website.

4. RPL in Practice: Evaluation of Prior Learning

Responsibility for submitting applications for the Recognition of Prior Learning rests with individual applicants. There is a detailed RPL application form and applicants will be interviewed by a member of the academic staff who will provide information and advice about the process. Each application must be accompanied by a completed RPL application form and evidence of prior learning e.g. transcripts of prior awards or certification.

4.1 Prior Certified Learning

Evidence of learning must be presented by the applicant in the form of official transcripts of results and formal syllabi accompanied by relevant supporting documentation. Recognition of prior certified learning is subject to evaluation by the Programme Director, who will take into account the student's academic record, course/programme of study, syllabus, course description, learning outcomes, number of contact hours, forms of assessment(s), NFQ level of qualification awarded (or equivalency).

4.2 Prior Experiential Learning

Where experiential learning is involved applicants need to present evidence of learning that demonstrate the achievement of learning outcomes of the relevant programme module(s). Candidates must demonstrate the appropriate academic level of learning as determined by the Head of School or Programme Director. This will normally involve candidates demonstrating that they understand the theory as well as the practical learning elements of a module.

A number of methods can be used to demonstrate the achievement of learning outcomes. These may include written evidence such as written examinations or essays, oral presentations, interviews, performance of set tasks, practical or written assignments or a combination of these. Assessment of prior experiential learning will be carried out by either the Head of School, Programme Director, or a member of academic staff competent in the subject area and then signed off by the Registrar.

The Registrar ensures that the RPL process is applied in a consistent, fair and transparent manner. This process is overseen by the Admissions Committee. Evidence submitted by an applicant is available for review by the External Examiner and the Admissions Committee.

4.3 Exemptions Policy for MBA

The College accepts that student participation forms a critical part of the Teaching, Learning and Assessment Strategy of programmes at Masters Level.

Therefore no module exemptions shall apply for the MBA programme. It is deemed to be in the best interest of the learners on the programme to implement this policy.

4.4 Validation

All RPL decisions must be validated and signed off by the Registrar.

All RPL recommendations and decisions are subject to audit by the Admissions.

4.5 Communication

All prospective applicants are made aware of RPL opportunities in programme literature and on the College's website.

Applicants will be fully informed of the application process, the stages within it and the nature and range of evidence that is considered appropriate to support a claim for Recognition of Prior Learning, including the learning outcomes against which prior learning will be assessed.

5. Review and Updating

This RPL policy will be subject to regular review and updating in line with emerging good practice and national and international policy updates.

AP 1.3a IBAT College Dublin English Language Recognised Equivalence

Minimum standards required in English for Academic Programmes

General or Academic English	Title of Award	**Minimum Level Required**
Academic	IELTS	**6**
Academic	ETAPP	**C1**
Academic	TOEFL https://www.ets.org/toefl/score-users/ibt/compare-scores.html	**iBT 60** **Historically:** **PBT 550** **CBT 213**
Academic	British Council -UCLES/IDP	**6**
Academic	JMB University Entrance test in English (Overseas)	**Pass**
Academic	AEB	**C**
Academic	OEB -English as a Foreign Language (Higher Paper)	**Pass**
General	TIE	**C1**
General	Council of Europe	**C1**
General	Trinity College (UK)	**10** **ISE – Level III**
General	TOEIC	**750**
General	London Tests of English (Edexcel) Pearson Language Assessment	**Level 4**
General	Cambridge ESOL CAE CPE	 **165** **Grade C**
General	Pitman UK	**Level 5 (Advanced)**
General	ARELS/Oxford UK	**Higher – Good**

Academic	Pearson Test of English	**46 or above**
Academic	Password Skills (for non-visa requiring students)	**Band 6**
Academic	DuoLingo Online English Test - From August 2022	**Score 105**
Academic	Oxford Test of English	**120**
General	Skills for English	**Minimum required: B2 Pass with Merit to equate to IELTS 6.0 or equivalent**
General	West African Senior School Certificate (WASSC - NFQ L4/5 equivalent) awarded by awarded by the West African Education Certificate (WAEC) and National Examination Council of Nigeria (NECO), applicable to only Nigerian and Ghanian applicants. Duration: The validity period of the WASSC must be within 5 years from date of application.	**Grade C6 in the English Language component**

AP 1.3b ATU English Language Recognised Equivalence

Qualification	Foundation	Undergraduate	Postgraduate
DuoLingo English Test (2021 Intake)	80	90 min 90 in each section	Min score 105, min 100 in each section
IELTS	5.0 (no band less than 4.5)	5.5 (no band less than 5.0)	6 (no band less than 5.5)
PTE Academic	< 51	51	55
TOEFL Paper	< 525	525	550
TOEFL IBT	< 70	70	80
TOEFL CBT	< 196	196	213
TOEIC	< 605	605	660
Cambridge Exam	< 173	FCE Grade C (173-179)	FCE Grade C (180-190)
Trinity College London		Trinity GESE 8 / ISE 11	Trinity GESE 9 / ISE 11
Qualifications must have been completed no more than 2 years prior to date that student will begin their studies e.g. for the September 2024 intake, applicants must have completed their English Language qualification in, or after, September 2022.			

https://www.lyit.ie/Study-at-ATU-Donegal/International-Students/English-Language-Requirements

AP 1.4 IBAT College Dublin Policy on Student Code of Conduct

IBAT College Dublin aims to provide a safe and welcoming environment for its staff and students and stakeholders. In order to achieve this, a standard of conduct is necessary on the part of students and staff. The purpose of this policy document is to outline the minimum standard of conduct expected by IBAT College Dublin in respect of its student body.

In order to ensure accessibility the Student Code of Conduct is available in Student Handbooks and via the IBAT College Dublin Portal.

The Student Code of Conduct is not a contractual document and is not intended to create legal rights or obligations whether contractual or tortuous or otherwise but it is written to foster an understanding between IBAT College Dublin and its students.

Terms

All students are expected to be considerate to the needs of fellow students, staff and any authorised visitors to IBAT College Dublin. As a basic minimum students are expected not to engage in any conduct which is intended or is likely to disrupt teaching, learning, study, research, events, recreational activities, meetings, examinations, administration or other activities. Above all students are expected to attend classes and fully commit to the learning process here at IBAT College Dublin.

Students are expected to respect the property of the College.

Student Misconduct (also refer to QAH, Chapter 7, Section 7.16 Student Disciplinary Committee)

Misconduct under the Student Code of Conduct is defined as improper behaviour such as interference with the proper functioning or activities of IBAT College Dublin, or those who work or study here, or action which otherwise damages the College or its wider reputation.

The following points are examples of misconduct. This list is not intended to be either exclusive or exhaustive:

- Disruption of the academic, administrative, or other activities of IBAT College Dublin, whether onsite or elsewhere.
- Obstruction of the functions, duties or activities of any student, member of staff or other employee of IBAT College Dublin or any authorised visitor.
- Use of violent, indecent, disorderly, threatening or offensive behaviour or language.
- Sexual, religious or racial harassment
- Fraud, deceit, deception or dishonesty in relation to IBAT College Dublin or its staff and students.
- Action likely to cause injury or impair safety on College premises
- Discrimination (under any of the nine grounds identified in Employment Equality Acts 1998–2015)
- Behaviour of a hostile or intimidatory nature
- Bullying in all its forms
- Abuse of alcohol or other substances on the College premises, in contravention of the regulations (regulations relating to the consumption of alcohol may change from time to time).
- Smoking in the College buildings in contravention of the Public Health Tobacco Act 2002, Section 47 (as amended) and the Tobacco Smoking (Prohibition) Regulations 2003.
- Damage to, or defacement of, College property or the property of other members of the College community, caused intentionally or recklessly, or misappropriation of such property

- Misuse or unauthorised use of College premises or items of property, including computer or network misuse
- Misuse of a Student ID Card, personation or activities involving false pretences or dishonesty.
- Misuse of official College documentation, including unauthorised amendment or defacement, or use or attempted use in a fraudulent or dishonest manner.
- Behaviour whether committed inside or outside the College which brings IBAT College Dublin, its students and/or staff into disrepute.
- Refusal to comply with any penalty (subject to the right of appeal applicable) imposed for offences.
- Incitement or encouragement of any other person to do any of the aforementioned things.

Failure to abide by Student Code of Conduct

A student who is suspected of breaching the Student Code of Conduct may be subject to the Student Disciplinary Procedure.

IBAT College Dublin

Code of Conduct

By registering with IBAT College Dublin you are signing up to a Code of Conduct that protects the College community. This code applies whilst you are on any of the College campuses or associated with any College activity on or off the campus. The purpose of the code is to ensure a safe and supportive environment for all members of the College.

You are expected to adhere to this Code of Conduct and any College regulations that apply to your programme as described in Quality Assurance Handbook (QAH). Please familiarise yourself with your Student Handbook and the College Policy on the Code of Conduct in the Colleges Associated Polices (page 27).

Where the code is breached you will be subject to the Colleges Disciplinary procedures as laid out in the Quality Assurance Handbook (section 7.16) and on the IBAT College website.

You are responsible for:

Engaging with your programme appropriately. This means:

- attending all timetabled activities
- coming to class, prepared, on time and with all relevant course materials
- actively engaging in class
- not engaging in other activities during class time

Respecting the learning environment by:

- being respectful to other learners, college staff and visitors.
- avoiding the use of abusive or hostile language, including body language.
- not using electronic devices for communication or non-class based activities while in class
- respecting college property and the property of others

You are also responsible for:

- familiarising yourself with all relevant regulations including the Policy on the College Code of Conduct and the Colleges disciplinary procedures which gives further information on what constitutes improper behaviour which may result in disciplinary action.

- reporting inappropriate behaviour such as discriminatory language, academic misconduct to protect the welfare of your fellow students and the reputation of the College.

AP 1.5 IBAT College Dublin Assessment Strategy

This document provides overarching principles to inform the development of programme and module assessment strategies. This document should be read in conjunction with:

- Assessment and Standards QQI Assessment and Standards Revised 2013
- IBAT QAH Chapter 8 – Assessment
- Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes
- AP1.15 IBAT College Dublin Blended and Online Learning Policy

IBAT is committed to ensuring that:

- learners have the opportunity to demonstrate their learning achievement
- assessment opportunities support standards based on learning outcomes
- assessment opportunities promote and support effective learning and teaching
- assessment opportunities are inclusive and support a diversity of learners
- assessment procedures are credible, i.e. fair, consistent, valid and reliable.
- assessment methods are monitored and reviewed as necessary to adapt to evolving requirements
- assessment requirements are explicit and accessible to learners at the commencement of the programme.

Adapted from QQI Assessment and Standards 2013

Assessment Supports Learning

Learners should have the opportunity to demonstrate they have achieved the intended learning outcomes.

Context

Each programme requires a programme, stage and a module assessment strategy.

These should be clearly articulated in the programme document. Where a programme has a special requirement that deviates from the institutional strategy or IBAT Assessment Regulations then those requirements must be clearly articulated in the programme document and in the programme assessment strategy. This should only be the case where a professional body recognition is contingent on a specific regulation.

The Approved Programme Schedule (QQI) or Programme Specification (UWTSD) is attached to the certificate of programme accreditation e.g. QQI Order of Council, and is deemed to form part of the assessment regulations applying to the programme. The Approved Programme Schedule is a summary of some of the information that should be in the programme assessment strategy. Any special assessment conditions (such as modules which cannot be passed by compensation) must be included in the Approved Programme Schedule. Such conditions must not contravene the Sectoral Conventions for Assessment (QQI Assessment and Standards 2013).

The assessment strategies presented for a programme or module must be transparent and accessible (published in programme documents and in module guides with reference to the appropriate grade criteria).

When articulated in an Approved Programme Schedule, assessment instruments are described as:

- Continuous Assessment (CA) *a piece of course work including in-class tests**
- Project /Dissertation
- Practical – *practical tasks, often assessed by way of a written report*
- Final Examination – *the terminal examination*

For the purposes of this paper an examination is defined as being conducted under Examination Office conditions. Class tests are deemed to be continuous assessment unless they are of the credit volume to warrant being held under examination conditions.

An assessment instrument is an assessment task, along with procedures for its conduct, together with the grading scheme and grade criteria.

Formative and summative assessment: All forms of assessment should be formative, where formative assessment is designed to provide constructive feedback. Purely formative feedback does not attract a grade. All assessment tasks that attract a grade are summative. The majority of assessment tasks at IBAT have elements of both formative and summative to varying degrees, for example a terminal examination is less formative than continuous assessment. See Glossary.

Overarching Principles of Assessment at IBAT

Assessment tasks are clearly linked to Learning Outcomes (LO).

A learner who achieves a pass grade in a module is deemed to have passed that module and achieved the minimum intended learning outcomes.

All assessment at IBAT is criterion-referenced assessment.

All assessment must be level appropriate, i.e. appropriate level indicators should be used as a guide.

The volume of assessment should match the effort hours as defined by the ECTS assigned to the module.

An element of early assessment with personalised formative feedback is especially important to learners in the earlier stages of a programme.

Appropriate and valid feedback should be available for all assessment tasks. The volume and detail of that feedback might vary on the scale from the detailed feedback required for an early piece of formative assessment in stage 1 to the less detailed rationale for a grade given on an award stage terminal examination.

Where a diagnostic assessment is used it should be formative and not attract a grade.

All programme assessment strategies are designed to:

- clearly articulate the assessment strategy in the context of the intended learning outcomes, skills acquired on the programme and graduate attributes.
- avoid over-assessment and duplication; there should be little if any overlap between intended learning outcomes across a level/stage
- ensure a balance of assessment within a stage.

Each module has a defined assessment strategy, there should be no changes to a modules assessment strategy or intended learning outcomes without being formally approved and applied to all programmes where the module may be cross-listed.

Where an 'integrated assessment strategy' is used it should be confined to one stage. The assessment instruments chosen should have component parts, the grades for each component should be attributable to a particular module and that component should assess at least one LO within that module.

Learners should be made aware of what constitutes academic misconduct and how to avoid it, learners should also be made aware of the consequences of engaging in academic misconduct.

All academic staff delivering on the programme, Internal Moderators and External Examiners should be supplied with the Programme Assessment Strategy and intended learning outcomes.

External Examiner(s) should be formally inducted to the programme prior to commencement of their duties. Where there is an External Examining team their tenure should be staggered to facilitate continuity.

A Programme Assessment Strategy

Each programme requires an assessment strategy; feeding into this overall programme assessment strategy are stage and module strategies (section B and C).

The Programme Assessment Strategy should be based on measuring the achievement of the Programme Learning Outcomes (PLO), it should also be clear how the assessment facilitates student learning by, for example, the quality of feedback and its relevance to improving learner achievement.

Any special requirements for the programme should be included in the programme assessment strategy e.g.

- Competencies within a module requiring a minimum pass grade
- A prescribed Examination: CA ratio required by a professional body.

Learners should be exposed to a variety and range of assessment instruments across a programme, this should be considered at the programme design stage and before individual module assessment strategies are devised.

Within the programme assessment strategy there should be a section on defining the approach to assessment at each stage. For example all assessment should:

- be appropriate to the level
- include level appropriate grade criteria
- have a balance of authentic assessment instruments within a stage
- have a balance of formative and summative assessment
- show progression from the previous stage (if appropriate)
- show how it is preparing learners for the next stage (if appropriate)
- at Award Stage the capstone strategy should be clearly defined and its assessment clearly articulated.
- if there is to be integrated assessment this should be clearly described in the programme assessment strategy.

Each Programme Intended learning outcome should be linked to a series of module intended learning outcomes which in turn are linked to a series of assessment instruments. This should be illustrated in the programme by way of a learning outcome matrix. This ensures assessment and therefore learning can be mapped to the appropriate award standard. Assessment supports standards.

The programme assessment strategy should clearly articulate synergy of assessment within a stage and progression between levels.

Assessment should be authentic, the programme assessment strategy should take account of measuring skills and competencies leading to our graduate attributes as well as the achievement of intended learning outcomes. To this end each programme should have a skills matrix. Skills can be assessed on the basis of basic (B), intermediate (I) or advanced (A). These should be linked to assessment instruments in modules across the programme, within and between stages.

All programme intended learning outcomes should be achievable by taking the core modules. If a programme intended learning outcome is only assessed via an elective it should be present in all electives.

Learners should be exposed to a variety and range of assessment instruments across a programme, this should be considered at the programme design stage and before individual module assessment strategies are devised. Programme assessment strategies should be reviewed periodically.

Summary:

When designing or reviewing a programme the following check list should be considered:

1. link the assessment tasks to the MILO and PLO.
2. describe the rationale for the selection of assessment instruments, criteria and procedures. It should address their fairness, consistency, validity, reliability and authenticity.
3. describe any special regulations

4. regulate, build on and integrate the Module Assessment Strategy.
5. provide contingent strategies – i.e. for learners with exemptions from RPL etc.
6. match the programme assessment instruments to the institutional grading requirements.
7. ensure that the programme's assessment load is balanced within a stage
8. relate the Programme Assessment Strategy to the Programme Learning and Teaching strategy

B Stage Assessment Strategy

At the early stages of a programme, early opportunities for formative feedback are particularly important.

At least one early diagnostic assessment should be considered per programme to identify where extra-curricular supports may be required.

A balance of formative and summative assessment should be achieved at each stage.

The variety and range of assessment instruments within a stage should be agreed before the module assessment strategies are devised, to avoid unnecessary duplication and to ensure that learners are not over-assessed.

Where integrated assessment is to be used it should normally confined within a stage or level and therefore be described on the Stage Assessment Strategy.

C Module Assessment Strategy

Each module requires a defined assessment strategy.

Each module intended learning outcome must be assessed at least once, but avoid over-assessment of intended learning outcomes.

The volume of assessment matches volume of effort as defined by the ECTS credit weighting of the module, IBAT define 1 ECTS as equivalent to 25 effort hours.

Each module assessment should refer to the programme and stage assessment strategies to:

- ensure that the assessment is level appropriate
- ascertain the type of assessment instruments to be used in that module,
- agree the balance of Coursework: Examinations etc.
- agree the appropriate balance of formative and summative assessment within the module
- agree which modules in a stage should have an early assessment instrument, or where diagnostic testing is to be used.
- agree which skills are being assessed in addition to, and in conjunction with, intended learning outcomes, for example a group work will assess the skill team work.
- also consider how the module relates to other modules within the programme –

1. Compare assessment instruments with related (e.g. co-requisites) modules within the level.

2. Ensure that the assessment is progressing from modules in the preceding level (pre-requisites) and preparation for the next stage where appropriate.

Module teams should remain current in terms of assessment methodologies and consider alternative types of assessment where and if appropriate. e.g.

- Self-assessment
- Peer assessment

Module teams should also consider their approaches to:

- Reassessment
- Alternative assessment where a learner may require reasonable accommodation – refer to IBAT College QAH.

Feedback

Feedback should evaluate the learner's performance regarding the assessment and be benchmarked against the published criteria.

Feedback should be returned within a specified time period and be formative. –"you can improve your grade by….", "you lost marks because…".

Feedback should be also have a positive element to indicate the strengths in assessment.

Feedback should explain how learners could improve their grades, where generic feedback is used this should be used in conjunction with personalised feedback.

Feedback should facilitate future learning (feed-forward), should encourage engagement with the assessor and where possible feedback should include feedback on the process as well as the product.

Each Programme Assessment Strategy should indicate the balance of formative and summative feedback this should include when feedback should be returned. All module guides should state:

- date of publication of the assignment
- submission date
- date feedback will be returned

For modules which culminate with an examination all continuous assessment must be returned to learners with grades and feedback at least two weeks before teaching ends.

For modules that are 100% continuous assessment, 70% of the continuous assessment must be returned at least two weeks before teaching ends.

See Also

- IBAT Grade Criteria
- IBAT Guidelines on Assessing Group Work

Summary of Institutional Norms

The effort hours associated with a module includes

- Class Contact (*lecture, tutorial, practical, seminar*)
- Assessment (*assignment and examination*)
- Placement
- Independent Work and evidenced self-study.

IBAT measures 1 ECTS as equivalent to 25 effort hours.

Where an unseen examination is used this is normally of 2 hours duration.

Practical's can be used to assess intended learning outcomes in the psychomotor domain (such as those concerned with attitudes or values) that are not easily assessed in examinations, presentation or *viva voce*.

A 5-credit module with a terminal examination should have at least one element of CA to provide early formative feedback and measure intended learning outcomes not easily assessed in a terminal examination.

A 10-credit module with a terminal examination should have at least one additional element of continuous assessment which allows for early formative feedback and the measurement of any intended learning outcomes not addressed in the terminal examination.

Where 10 credit modules with terminal examinations are used in stage 1, a selection of those modules usually have an in-class test at the end of semester 1. In addition they should have at least two additional elements of continuous assessment one of which allows for early formative feedback.

The weighting of the examination relative to the continuous assessment should depend on:

- the stage in the programme, the balance normally shifting in favour of examinations as approaching the award stage. A terminal examination of 2 hours duration would normally account for not less than 50% of a 10 credit module.
- the appropriateness of the assessment instrument to measure the MILO
- any special considerations in the Approved Programme Schedule

Within an examination the number of questions should be considered in the context of the depth and breadth of material being assessed in the examination. Compulsory questions are appropriate in the context of assessing minimum intended learning outcomes.

Glossary

See also QQI Assessment and Standards 2013

Authentic Assessment

Authentic assessments test student abilities by measuring how well learners perform under real-life or simulated contexts.

Authenticity is related to validity. Authentic assessment involves using assessment tasks that resemble the kinds of professional tasks that arise in the relevant community of practice. The assessment task must appear authentic to the learner. Examples include the use of a poster presentation or the writing of a short research article as part of the assessment task for a final-year investigative project. These are authentic because they are typical communication channels for researchers.

Constructive Alignment

Constructive alignment ensures that there is a clear relationship between learning outcomes and assessment.

The main steps in the alignment process are:

- Defining the intended learning outcomes
- Choosing teaching/learning activities likely to help and encourage learners to attain those objectives
- Engaging learners in those learning activities through the teaching process
- Assessing students' learning outcomes using methods that enable learners to demonstrate the intended learning and evaluating how well they match what was intended
- Arriving at a final grade, and perhaps in the case of formative assessment, giving feedback to help learners improve their learning.

Criterion Referenced Assessment

Each student's achievement is judged against specific criteria. In principle no account is taken of how other learners have performed. In practice, normative thinking can affect judgements of whether or not a specific criterion has been met. Reliability and validity should be assured through processes such as moderation, trial marking, and the collation of exemplars.

IBAT Colleges Grade Criteria have been informed by the NFQ Grid of Level Indicators (https://www.qqi.ie/Downloads/NFQLevelindicators.pdf) and developed by the academic team, Academic Director(former) and Registrar.

Diagnostic Assessment

Like formative assessment, diagnostic assessment is intended to improve the learner's experience and their level of achievement. However, diagnostic assessment looks backwards rather than forwards. It assesses what the learner already knows and/or the nature of difficulties that the learner might have, which, if undiagnosed, might limit their engagement in

new learning. It is often used before teaching, or in the early stages of a module or programme to indicate if additional supports are required.

Formative Assessment

Formative assessment* is an integral part of teaching and learning. It does not contribute to the final mark given for the module; instead it contributes to learning through providing feedback. It should indicate what is good about a piece of work and why this is good; it should also indicate what is not so good and how the work could be improved. Effective formative feedback will affect what the student and the teacher does next.

Summative Assessment

Summative assessment* demonstrates the extent of a learner's success in meeting the assessment criteria used to gauge the intended learning outcomes of a module or programme, and which contributes to the final mark given for the module. It is normally, though not always, used at the end of a unit of teaching. Summative assessment is used to quantify achievement, to reward achievement, to provide data for selection (to the next stage in education or to employment). For all these reasons the validity and reliability of summative assessment are of the greatest importance. Summative assessment can provide information that has formative/diagnostic value.

***Note: At IBAT to encourage learners to participate in all assessment tasks we prepare tasks that have elements of both formative and summative assessment i.e. they attract formative feedback and a mark.**

Integrated Assessment

For the purposes of this document integrated assessment is a single piece of assessment that is assessing the learning outcomes of more than one module.

AP 1.5b Assessment Workload Guidelines

1 Introduction

This document is the start of an exercise to provide a set of guidelines for academic staff developing programmes and modules at IBAT College Dublin. The project is in response to a 'call on institutions to further link study credits with both learning outcomes and student workload and to include the attainment of learning outcomes in assessment procedures' – Bucharest Communiqué, 2012 as articulated in the ECTS Users Guide 2015.

Purpose: To ensure that the constructive alignment of the key curriculum elements: Minimum Intended Module Learning Outcomes, teaching and learning activities, and assessment tasks are properly balanced and practically applied across the programme an understanding and recognition of the assessment workload is required.

In summary the aims of these guidelines are to:

- Ensure that the assessment workload is appropriate to demonstrate the achievement of the Minimum Intended Module Learning Outcomes
- Ensure an appropriate balance of assessment workload within a programme
- Ensure that there is a correlation between workload and ECTS and that it is appropriate
- Incorporate learner effort including word count considerations into assessment design
- Provide guidance to academic staff when designing the module assessment strategy at the programme development stage
- Assist new or less experiences academic staff in setting assessments.
- Provide an indication to learners of the relative effort required to complete an assessment - linked to the credit value of the module

This paper is informed by research reported at UCD, in particular the research carried out by Noonan and O'Neill on student engagement and the first year experience. The workload equivalencies have been informed by a series of work load equivalence tables from UK HEI's and references cited therein. Where there is significant disparity a judgement was taken and agreed internally. It is acknowledged that word count equivalence, although traditionally used as a workload indicator, is challenging to apply to the variety of authentic assessment instruments employed in modern programmes.

These guidelines will inform a 'programme approach to assessment' intended to ensure consistency across the programme leading to a coherent learning experience, balanced assessment and the avoidance of over assessment.

At a modular level the Six Module Design Principles (O'Neill and Noonan, 2011) are recommended:

1. Allow students, where possible, have opportunity for regular, low stakes assessment with opportunity for feedback on their progress.
2. Develop students' opportunities for in-class self and/or peer review of their learning against assessment criteria.

3. Allow students multiple opportunities for well-structured and supported collaborative learning and its assessment (peer and group-work, project work).
4. Consider the redesign of the learning sequence of module learning activities in an efficient and effective manner, including the related blended learning opportunities.
5. Introduce more active/task-based learning which uses more authentic assessments i.e. subject/ discipline identity).
6. Consider the student work-load demands within the module, as well as in parallel modules.

In addition, and with Ref to IBAT College Assessment Strategy AP1.5 – Include appropriate integrated assessment opportunities where integrated assessment is a single piece of assessment that is assessing the learning outcomes of more than one module.

2 Recommendations

Tutorials should include opportunities for early formative feedback, the effort expended, by a learner on preparing for a tutorial should be estimated at 10 hours per hour-long tutorial, this should not be included in the assessment count unless a summative element is included.

Normally 20% of the notional workload should be assigned to assessment. Assessment workload includes; reading, gathering and organising information, drafting, editing, and delivery (presentation or completing an exam).

- 25-30 hours for a module worth 5 ECTS
- 50-60 hours for a module worth 10 ECTS

Normally no more than 2 discrete pieces of assessment for 5 ECTS module at level 6/7 unless justified for sound pedagogic reasons and included in the module descriptor.

Assessment	**Effort Hours**	**L6/7/8 5 ECTS**	**L6/7 10 ECTS**	**L8 10 ECTS**
3 Hour Exam (unseen)	**30**	N/A	N/A	50%
2 Hour Exam (unseen)	**20**	*60%*	*40%*	*40%*
1 Hour Class Test (unseen)	**10**	*30-40%*	*20%*	*20%*
1 Hour MCQ (unseen)	**10**	*30-40%*	*20%*	*20%*
Essay 1000 (seen)	**10**	*30-40%*	*25%*	*25%*
Essay 1500 (seen)				
Assignment 2000 (seen)	**20**			
Proposal/portfolio/ small project 3000-4000	**30**	*N/A*	*100%*	*60%*
Group Assignment 800-1000 words each	**10**	*30-40%*	*20%*	*20%*
Project -6000 -8000	**50**	*N/A*	*100%*	*100%*
Individual or Group Oral Presentation	**5**	*15- 20%*	*10%*	*10%*

Individual or Group Poster Presentation	**10**	*30%*	*20%*	*20%*

For Example: L7 10ECTS module has 50 hours attributed to assessment. This is made up of: 1 mid-sessional In-Class Test, 1 CA comprising 2000 words and 1 two hour exam.

3 References

ECTS Users Guide 2015 – European Commission

Student Engagement and Assessment: The First Year Experience - Elizabeth Noonan and Geraldine O'Neill - University College Dublin

Hornby, W (2003) Strategies for Streamlining Assessment: Case Studies from the Chalk Face

Assessment Of/For/As Learning – National Forum Resources

Assessment Equivalence Tables from:

- UWTSD
- University of Ulster
- Manchester Metropolitan
- London Southbank University
- Edinburgh Napier University
- Glasgow Caledonian University

AP 1.6 IBAT College Dublin Teaching and Learning Strategy

This strategy lays out the priorities for developments in Teaching and Learning at IBAT College Dublin. The strategy is overseen by the Teaching and Learning Committee reporting to the Academic Council. This document has been informed by:

1. College Strategic Priorities (Section 1.6 QAH)
2. Quality Enhancement Plan
3. Educational Philosophy (Section 6.1 QAH)

1. The College Strategic Priorities include the development of more industry informed programmes, enhancing the learner experience and progression and promoting excellence in teaching and learning.

2. The three year Quality Enhancement Plan is laid out under the following themes:

1. Teaching and Learning Strategy
2. Better Quality Student Engagement
3. Benchmarking Performance
4. Academic Staff Development
5. Enhancing the Learning Environment

The plan includes a range of initiatives including:

- Prioritise retention, progression, programme completion and awards
- Involve learners in deeper, more comprehensive consultation on policy and process
- Ensure support is available to encourage uptake of technology enhanced learning supporting the Teaching and Learning Strategy.
- Improve the College engagement with the National Forum for the Enhancement of Teaching and Learning in Higher Education
- Improve Staff qualifications in teaching and learning
- Enhance and demonstrate staff engagement with Scholarship
- Improve Library provision and ensure library resources are available for day, evening and weekend learners.

3. The Educational philosophy is that all programmes are aligned to the National Framework of Qualifications and are underpinned by a learning outcomes approach to all modules and programmes, clearly describing what a graduate is expected to know, understand and be able to demonstrate after completing a process of learning.

These commitments, plans and aspirations have been translated into the following Teaching and Learning Strategy:

1. The College will undertake widespread development in the design of effective **learning outcomes**, appropriate learning activities and constructively aligned assessment. Having a well-defined and clearly articulated set of learning outcomes is vital to provide

learners with a clear purpose to focus their learning efforts and guide academic staff. This supports the Colleges programme development agenda.

2. **Staff development** underpins the colleges teaching and learning agenda. In addition to improving formal staff qualifications in teaching and learning, greater engagement with organisations such as the National Forum [1] will be facilitated to ensure staff are familiar with new initiatives in teaching and learning and encourage implementation where they add value. This includes greater integration with the library service and the incorporation of information literacy and other supports into the curriculum.

3. The College strategic mission to offer **industry-relevant programmes** and enhance graduate employability will be achieved by working closely with the Business Advisory Group (BAG) to inform programme design, the development of graduate attributes, identifying relevant skills and competencies and support in identifying authentic learning activities and authentic assessment.

4. Enhancing the learning environment including the virtual learning environment will involve exploring **technology enhanced teaching and blended learning** opportunities. This will also support building digital capacity aligned with the themes of the National Forum[2].

5. The development of programmes and their delivery will be informed by the principles of **instructional design**, this theme will inform staff development and also support the development of blended learning.

6. IBAT College Dublin has traditionally attracted a significant cohort of international learners, has built up an expertise in teaching and supporting international learners and benefits from a diverse learning environment. To build on this capacity and as part of the programme development agenda the college will work on **the internationalisation of the curriculum[3]** for the benefit of all learners and to produce globally relevant graduates.

7. This strategy will ensure that **learner analytics** and the data collected from self-monitoring activities and the Colleges retention strategy, such as retention data, learner satisfaction, awards and graduate outcomes are used to measure the effectiveness of the strategy and teaching and learning initiatives in general.

8. Aligned with the Hunt Report[4] principle that "*Every student should learn in an environment that is **informed by research, scholarship and up-to-date practice and knowledge***" this strategy includes an aspiration to develop initiatives to ensure and measure staff engagement with scholarship to inform their own academic development and teaching practice.

9. To ensure that the learner is at 'heart of everything we do' **greater learner engagement** with College governance is necessary. This will go further than learner (and alumni) membership of relevant Board and Committees to include training and development to ensure learners can be partners in influencing the College's strategic direction and to ensure that the learner influence is sustainable.

REFERENCES

1. National Forum for the Enhancement of Teaching and Learning in Higher Education - *www.teachingandlearning.ie*

2. Towards a National Digital Skills Framework for Irish Higher Education - University of Limerick 2015

3. Irish Educated Globally Connected, an International Education Strategy for Ireland 2016-2020

4. National Strategy for Higher Education to 2030 (Hunt Report)

AP 1.7 IBAT College Dublin Quality Enhancement Plan

IBAT College Dublin

Quality Enhancement Plan

The IBAT College Dublin Quality Enhancement Plan is informed by its strategic planning and by a series of recent reviews of IBAT College Dublin (including programme validation events) and staff, learner and industry consultation. The plan is a three year plan with phase 1 being a review of the effectiveness of our revised Quality Assurance polices and processes.

The plan is under development and subject to the approval of the Academic Council and to be endorsed by the BoG. Once approved, progress will be reported to the Audit Sub-Committee and to each Academic Council.

1. **Teaching and Learning Strategy**

Aim: to produce a comprehensive and effective Teaching and Learning Strategy aligned to IBAT's Strategic Plan and designed to support the IBAT mission to produce graduates who are industry focussed, socially responsible and globally relevant.

Themes 2017/18:

- Further development of Teaching and Learning Strategy/ educational philosophy
- Skills for employment (employability audit on new programmes)
- Business Advisory Group to inform programme design and development of graduate attributes.
- Blended learning- technology enhanced teaching -where it adds value

2. **Better Quality Student Engagement**

Aim: to enhance the quality of learner engagement with the College in all aspects of College life.

Themes 2017/18:

- Class Representatives training introduced
- Learners involved in deeper, more comprehensive consultation on policy and process

This will be measured, in the first instance, by improved attendance by learner representatives at Boards and Committees and quality of feedback from consultation exercises.

Themes 2018/19:

- Alumni engagement – first destination survey introduced in Dec 2017.

3. **Benchmarking Performance**

Aim: To ensure through effective process, reporting and analysis that IBAT College Dublin identifies areas of good practice and areas for improvement. Benchmarking against similar

providers, nationally and internationally to be undertaken, and the production and use of key performance indicators (KPIs) for internal improvement. Current benchmarking exercises include:

- Student Staff Ratio
- Retention, Progression, Completion and Awards

4. Academic Staff Development

Aim: To ensure IBAT learners learn in a research informed environment and have access to effective teaching and learning methodologies.

- Improve Staff qualifications in T&L
- Improve the College engagement with the National Forum for the Enhancement of Teaching and Learning in Higher Education
- Enhance and demonstrate staff engagement with Scholarship
- Support Continuous Professional Development initiatives undertaken by academic staff

5. Enhancing the Learning Environment

Aim: to ensure IBAT College Dublin learners are learning in a high quality learning environment with effective learning resources. This project will commence with an evaluation of the effectiveness of IBAT facilities for the delivery of all programmes of Higher Education and Training

- Ensure facilities are appropriate, maintained and provide a conducive learning environment
- Improve Library provision and ensure library resources are available for day, evening and weekend learners.
- Information Technology – ensure support is available to encourage uptake of technology enhanced learning supporting the Teaching and Learning Strategy.

References:

IBAT Reports and Action Plans

National Strategy for Higher Education to 2030 (Hunt Report)

Quality in an Era of Diminishing Resources' Irish Higher Education 2008-15 - QQI March 2016

Review of Reviews QQI 2014

Towards a National Digital Skills Framework for Irish Higher Education - University of Limerick 2015

AP 1.8 Human Resources Policy for Staff Recruitment, Management and Development

IBAT College Dublin considers the quality of its people to be a critical success factor, which includes the capacity to attract, develop and retain management and staff with the necessary talent and expertise required to support the continuing academic and commercial development of a successful organisation. IBAT College Dublin is committed to the timely selection of employees in a consistent and professional manner throughout the organisation irrespective of age, race, gender or disability. The college strives to ensure provision of job satisfaction, professional development, career advancement and fair financial rewards within a progressive educational environment.

1. Staff Recruitment

The decision to recruit an employee is made in response to an identified need within the College. The needs of the organisation are reviewed annually as part of the planning process.

When the need for a new employee is identified a job analysis, job description and person specification are produced. A job analysis is performed to clarify the duties, responsibilities and other job demands of each role. It helps to identify the ideal employee profile to satisfy the needs of the organisation. The job description outlines the goals and objectives of the job including the main activities and reporting relationships involved in its performance. The job description is sufficiently flexible to allow the roles, tasks and responsibilities to evolve. The person specification sets out the requirements of the job in terms of qualifications, personal skills, and experience.

Selection procedures commence at this stage. A hiring strategy is formulated, a job specification is prepared and the position is advertised, applications from internal candidates are also considered. All CVs based on the job criteria are reviewed to identify potentially suitable candidates.

The job interview is the primary selection method used to assess candidates' suitability for a particular post. Interviews are conducted in a professional, fair and consistent manner. A minimum of two interviews, with a panel of (a minimum of three) interviewers – to include the line manager, are conducted to reduce potential bias in the interview process. The College expects all interviewers to be adequately prepared for the interview process; therefore, each interviewer is required to know the specification for the job they are interviewing for. The use of clear interview notes on each candidate is an absolute requirement.

The decision to hire a candidate is made by consensus of the interviewers. Candidates are ranked in terms of suitability and the process proceeds to offer stage with the most suitable candidate.

2. Employment Offer Generation

When a suitable candidate is identified the following procedures must be followed prior to an offer being extended

- A background check should be completed to verify candidate details
- Professional references, including phone numbers of suitable referees, are obtained from the candidate (at least one reference from a former line manager).
- Authenticated copies of academic transcripts.

3. Extending an Offer of Employment

When a suitable candidate is identified and when all of the pre-hire activities have been completed satisfactorily, an Offer of Employment is extended verbally to the successful candidate by the Direct Manager. A formal Letter of Offer, including the Statement of Terms and Conditions of Employment, is sent to the successful candidate. The candidate must respond within seven days of receipt of the offer. The offer may be withdrawn if the candidate does not meet this requirement. A file must be completed on both successful and unsuccessful candidates. Successful candidate files should contain:

- Candidate's most recent CV
- All interview notes
- Completed and signed contract of employment.

4. Recruitment Code of Conduct

To avoid any real or perceived conflict of interest, company personnel involved in the hiring process, should avoid interviewing and/or making hiring decisions which involve family members, relations or friends.

5. Procedure for Induction

Fast and effective assimilation of new employees into the organisation is a priority. All new staff must complete a company Induction and Orientation programme. The following are the primary components of this programme

- Introduction to the organisation including background, ethos, structures, strategies and plans

- Academic and administration procedures and regulations (including equality and diversity policy)
- Roles and responsibilities of academic staff, including pedagogical expectations, teaching, learning and assessment strategies, engagement with training and CPD
- Terms and conditions of employment
- Overview of the IT system
- Overview of safety requirements

The College Director is responsible for ensuring that induction and orientation is provided for each new hire, and for internal staff movement, and this responsibility is fulfilled operationally through functional heads.

6. Career Development

Within the context of the College's Staff Development Policy all staff are encouraged to prepare, plan and consider their own career development, considering particularly activities which will support IBAT College Dublin's Teaching, Learning and Assessment strategy.

In accordance with the College's staff recruitment and development policy, new permanent full-time academic staff appointees, who do not hold a recognised framework-aligned qualification in Learning, Teaching and Assessment, are required to undertake one within a time frame agreed with the Head of School. Part-time academic staff appointees, who do not hold a qualification in Learning, Teaching and Assessment will be supported to undertake such qualification with the agreement of the Head of School and in line with their terms of employment.

Conditions governing staff access to career development does not discriminate, directly or indirectly, on any of the nine grounds of the Employment Equality Acts 1998–2015, as outlined above.

7. Staff Communication

IBAT College Dublin recognises the education and organisational benefits of having a diverse community of staff and students and continues to build and maintain an inclusive environment which promotes equality, values diversity and respects the rights and dignity of all.

The College is committed to this Equality and Diversity Policy which embodies non-discrimination towards all employees, applicants for employment, and students. To this end, IBAT College Dublin aims to ensure that all individuals (employee, potential

employees and students) are treated fairly and equally, with dignity and respect irrespective of their:

- Gender
- Civil (marital) status
- Family status
- Sexual orientation
- Religion
- Age
- Disability
- Race
- Membership of the Traveller community

8. Objectives of Equality Planning

The purpose of the Equality/Diversity Policy is to promote an affirmative place of learning and work that provides for equal opportunities for all current, future and potential staff and learners and where their dignity is protected and respected at all times.

9. Responsibility

IBAT College Dublin is committed to the active implementation of this equality/diversity policy. College senior management have responsibility for ensuring the implementation of the policy in the workplace and promoting a culture that supports the policy.

All employees receive a copy of this policy and staff training is also provided, in particular to new staff. This includes the provision of an interactive workshop in Multi-culturalism. This session provides insight into cultural differences and their implications, how to deal and communicate effectively with learners from different cultures, and the challenges and benefits of cultural diversity within the College.

10. Recruitment and Selection

The objective is to target the widest possible pool of potential applicants and to ensure that all candidates have equal access to the College's positions. Recruitment methods, documentation and all associated publicity material are reviewed to ensure it contains nothing of a discriminatory nature and encourages applications from all potential candidates.

Selection is based on merit and those who are successful demonstrate their suitability for appointment according to predetermined job-related selection criteria which is consistently applied throughout the recruitment process. The application of the equality/diversity policy also includes accommodating as much as possible the special needs of individuals to facilitate their participation in the recruitment and selection process.

All aspects of the recruitment and selection process (job description/specification; advertising; short listing; interviewing; reference checks) are based on the principle of assessing competencies and attributes (abilities) of applicants against those which have been determined to be required for the effective performance of the job.

11. Conditions of Employment

All employees receive the same treatment, in relation to disciplinary measures, grievances, etc., irrespective of their campus location.

The induction process is used as an opportunity to discuss with new employees any special needs that they may have arising from one of the nine grounds identified in the Employment Equality Acts 1998–2015, and to explore how these needs may be accommodated. Where practicable, measures are taken to accommodate special needs arising from a disability, race, family status, or any other characteristics covered by these nine grounds. For example, requests for flexible working hours/atypical attendance patterns are accommodated where practicable.

12. Role of Staff

All staff have an important role to play in ensuring equality/diversity throughout the College, and have a particular responsibility to engender respect for difference and to accommodate diversity, where/as appropriate.

Additionally IBAT College Dublin staff are required to support the College's commitment to maintaining a work and academic environment free of harassment and bullying.

13. Equality Training

All staff receive training on the equality and diversity policy at their induction, and whenever updates are made to the policy in this area, and are aware of the College's equality/diversity principles, the relevant legislation, and senior management/staff commitment and responsibilities in implementing the policy.

14. Staff Appraisal

The formal staff appraisal process within IBAT College Dublin supports the review of performance of roles, the achievement of goals and objectives, and the implementation of staff development plans by line managers. It also focuses on future goals, objectives and development plans in the context of evolving operational responsibilities and career development.

The Staff appraisal process is managed through an easy to use team performance management system application.

On an annual basis, at a minimum, the College Director, in consultation with the Senior Management Group, sets goals for the organisation based on the output of the business planning process. Each line manager then sets:

- individual goals and objectives for each employee
- individual development plans are formulated, negotiated, approved and implemented in support of the achievement of these goals– through the use of the performance management application.
- semi-formal reviews, are carried out to review progress and updates based on evolving business plans and objectives – through the performance management application.
- formal annual appraisal – utilising the performance management application to facilitate the meeting.

AP 1.9 College Data Protection and Record Management Policy

Overview and Objectives

Data Protection is the safeguarding of privacy rights of individuals in relation to the processing of personal data. Data Protection legislation regulates the collection, processing, keeping and disclosure of personal data and to give individuals access to their data. IBAT respects the privacy and Data Protection rights of its students, staff and other persons it holds data of by complying with its obligations under such legislation. The following are the current legislation governing data protection and the processing of Personal Data:

- The Data Protection Act 1998 (The Principal Act)
- The Data Protection (Amendment) Act 2003
- The Data Protection Bill 2017, and any subsequent published Act
- The General Data Protection Regulation (GDPR) May 2018
- ePrivacy Directive May 2018

Legislation sets out the rules about the way in which personal and sensitive personal data is collected, accessed, used and disclosed. Individuals have the right to access their personal data on request and the right to have their personal data amended if found to be incorrect.

This policy states IBAT's policy for compliance with Data Protection legislation. Appendix 3 is a glossary of terms to assist explaining terms contained in the legislation.

IBAT College is a Data Controller with certain staff acting as data processors. The Registrar is the main point of contact within the college for data subjects (staff, students and the general public).

Current Data Protection legislation will be superseded by the General Data Protection Regulation (GDPR) from 25th May 2018.

The GDPR defines personal data as:

> *Any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, and bank details, your posts on social networking websites, your medical information, or your computer's IP address*.

The GDPR defines special category data (previously known as sensitive personal data) as:

> *racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; biometric data where processed to uniquely identify a person.*

Some of the key changes in the GDPR are listed below:

- Change to the definition of consent – Must be 'unambiguous' so no opt-outs or pre-ticked boxes, this includes sending of marketing such as newsletters to alumni. Consent must also be obtained for each distinct use of an individual's data (you can no longer package together multiple uses), and must be able to be withdrawn easily.
- Consent must be unambiguous, freely given, specific and the data subjects should be informed for each purpose for which the data is being processed, especially if the purposes evolve overtime.
- 'Explicit' consent must be received for transferring personal data outside the European Economic Area (EEA) and specific safeguards need to in place to facilitate such transfers.
- Privacy notices must be provided and must contain specific information, including details of retention periods and the legal basis for processing.
- Data breaches must be reported to the Information Commissioner within 72 hours.

- Data Protection Impact Assessments (risk assessments) must be completed for all new high risk processing e.g. anything with sensitive data such as health related information that identifies living people.
- Profiling requires consent e.g. Learning Analytics. This refers to use of so called 'big data' and using information to predict behaviours.
- The time limit for providing access to an individual's personal data changes from 40 days to 30 days (with an extension possible in some specific cases).
- Data processors (companies or individuals providing processing of personal data on behalf of a data controller) will be liable for their actions i.e. capable of being fined as well as the data controller, contracts should reflect these new responsibilities.
- Data controllers are required to document how they are compliant with the Regulation. Part of this requires the creation of a register of personal data assets held, showing what personal data is collected, how it is used, how it is secured, whether it is shared and how long it is retained.
- Under the GDPR, data subjects will have the right to withdraw their consent at any time. Mechanisms should, therefore, be in place to ensure that the process is both simple and effective, they should also be informed of this right prior to giving their consent.
- The GDPR largely preserves the current Data Protection Acts with regard to overseas transfer of personal data, for example, prohibiting transfers of personal data outside of the EEA unless certain conditions are met (adequacy).
- Introduced the role of the Data Protection Officer (DPO) under Article 37, an independent and leadership role responsible for overseeing data protection strategy and implementation to ensure compliance. Article 39 outlines a DPOs responsibilities.

2. Scope and Applicability:

This policy applies to staff (including contractors, e.g. agent, not in the college and temporary staff in the college) setting out the policies and procedures when dealing with data. The Data Protection and Retention Policy ensures that the College has a systematic approach to comply with any laws, regulations and quality assurance policies, it also assists and informs staff about their duties and makes it clear the procedures for collecting, storing and processing data.

3 Collecting information

IBAT collects and uses data from the general public, students and staff to provide the following services;

To the public

- Provision of progamme information to the general public.

Students

- Application and registration of students.
- Payment of fees.
- Enrolment for examinations.
- Identification of student educational requirements
- Assessment details and award classifications
- Information about qualification(s) attained or for any other purposes to third parties, e.g. from time to time, IBAT disclose personal data to third party agents who provide products or services to the College, for example, student data may be given to photographers for photo-shoots (with prior consent from the student).
- Information to regulatory bodies e.g. Quality & Qualifications Ireland (QQI) or
- Information to accreditation bodies (University of Wales (UoW) / Trinity Saint David (TSD)) or
- Information to professional bodies if students pursue on-going professional exams.

Information is only released with the explicit consent of the student. In the case of information to QQI and accreditation bodies this is provided at registration stage.

Staff (including temporary staff, External Examiners, lecturers, contractors etc.)

- To perform accounting, personnel, payroll, pensions and other record keeping functions

All services comply with our legal obligations

The Registrar is obliged to transfer data to other organisations for regulatory and accreditation purposes. The table below outlines in brief who these organisations are the nature of the data transferred

Organisation	Type of data
Quality & Qualifications Ireland (QQI) – Dual mandate of Regulator of the further and higher education sector and Validation of Programmes and awarding of qualifications.	Currently as there are no admissions on the QQI validated programme data is entered on the QQI system, QBS to enable awards to be run. Going forward, subject to a successful re-engagement and validation of future programmes, data will be furnished to assure QQI that the academic standards required are maintained in any QQI validated programme; Data shared includes people registered on validated programmes, progression data, completion and attrition data etc.
University of Wales/Trinity Saint David Validation	Student registration details and exam results are uploaded in a file format prescribed by UoW TSD. They are uploaded to a university portal for consideration by UoW TSD. In addition to the sharing of personal data there are reports and statistics provided reviewing the programme annually.
HEA	Aggregate data, no personal data is provided. For example, number of students enrolled in the college, number enrolled on a particular programme, demographic data – e.g. nationality, gender etc.
Garda Siochana	Personal details of enrolled international students that require a visa to study must be provided in a Garda Siochana approved template (GN1B).

4. Data Protection Rules

IBAT performs its responsibilities as a data controller under the legislation in accordance with the eight principles of Data Protection, which are;

4.1. Obtain and process the information fairly

IBAT obtains and processes personal data fairly and in accordance with statutory and other legal obligations.

4.2. Keep it only for one or more specified, explicit and lawful purposes

IBAT retains personal data for purposes that are specific, lawful and clearly stated. Personal data is only processed in a manner compatible with these purposes.

4.3. Use and disclose only in ways compatible with these purposes

IBAT discloses personal data only in circumstances that are necessary for the purposes for which the data is collected. Where personal data is used for marketing purposes, appropriate consents must be obtained from data subjects.

Where prior notification and or consent is required and is provided by data subjects, IBAT may disclose information to its agents, advisors, service providers and contractors for the following purposes:

- Processing and accessing student examination applications.
- Attendance at lectures or other events hosted by IBAT or in conjunction with its education partners, e.g. QQI, UWTSD.
- Identifying educational requirements.
- GN1B Information to Garda for the purposes of inbound international students..
- Verifying personal data, including for staff recruitment contacting prior employers or professional advisors.
- Meeting IBAT's legal obligations including payroll.
- Marketing purposes, if appropriate consent is received.

4.4. Keep it safe and secure

IBAT will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of personal data and against accidental loss or destruction. This includes adopting enhanced security measures, if appropriate, where personal data is being stored or processed outside IBAT office locations.

The IT department configures all network and smart devices (whether desktop PC, laptop, smart phones, tablets, etc.) with the appropriately security standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.) to ensure the security and privacy of data within the organisation.

All wireless technologies/networks used to access the systems within IBAT College Dublin are encrypted.

IBAT College Dublin ensures that all staff are aware of security measures and comply with them such as:

- Personal electronic data should be subject to stringent controls, passwords, encryption, access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data, should not be visible to unauthorised persons.
- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PCs, ensure the hard drive is cleaned (i.e. all personal data is removed) by an appropriate IT staff member.
- Special/appropriate care is taken where laptops and PCs containing personal data are used outside the College. All staff are aware of the potential risk this presents and manage the risk accordingly.
- Health and student welfare support personal data can only be released following consultation with the relevant professional.

4.5. Keep it accurate, complete and up to date

To ensure high levels of data accuracy, completeness and ensure personal data is up to date. IBAT procedures will include providing online access to students to their personal data and permit them to amend their data pertaining to personal contact details. There have no access to examination data..

4.6. Ensure it is adequate, relevant and not excessive

IBAT will only request and retain personal data to the extent that there is a demonstrable business or education need and will ensure that it is adequate, relevant and not excessive.

For example - The College uses email and a SMS text messaging system which allows authorised staff to communicate with students quickly and comprehensively. Registered students will be automatically added to the list to receive emails and texts regarding college-related information. This may include, for example, if lectures have been cancelled or rescheduled at short notice, reminders related to examinations, details regarding library loans and renewals etc.

4.7. Retain for no longer than necessary

IBAT maintain a data retention schedule (**Appendix 1** of this policy) which documents the retention period for all data (including personal data). The retention schedules will be reviewed annually by those responsible for the particular data sets, e.g. Finance data by the Accountant, Academic data by the Registrar, Head of School depending on the nature of the data. It will be amended if necessary. Records, including personal data will be purged in line with the retention policies.

4.8. Give the member a copy of their personal data on request

IBAT procedures ensure that students and staff can exercise their rights under legislation to access their data. When a request is made, either in writing or my e-mail, the data that is processed on their behalf, along with a description of the data and the reason for processing is furnished.

5. Disclosure of personal data

The legislation recognises two categories of Personal Data –

- 'Ordinary' Personal Data, such as name, address, mobile phone number, car registration, PPS Number.
- Sensitive Personal Data, which is more deeply personal to an individual, such as their racial or ethnic background, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the (alleged) commission of any offence, subsequent proceedings or sentence. Exam results are treated as sensitive data and access is restricted with increased security to such data.

Sensitive personal data should normally only be processed if the data subjects have given their explicit consent to this processing.

The legislation applies equally to automated and manual data, i.e. data held or processed on a computer, or data held in 'hard copy', stored in an indexed or relevant filing system.

The security of personal information in the possession of the College is of paramount importance and is, therefore, addressed in various policies and procedures throughout the College, e.g. the Quality Assurance Handbook, the College Risk Register and this policy.

In addition to the principles contained within this policy, staff and students are also advised to adhere to the Password and File Management practices in the college.

5.1 Provision of access to third parties

It is not IBAT College Dublin policy to contact a student or staff member on the basis of a request from a third-party, and a third-party who contacts the College to express concern about the welfare of a student or staff member should also be informed of the following policies.

- A third-party must not be given a student's or staff member's address or telephone number. However, where a third-party is seeking to contact a student / staff member, it is appropriate to ask the third-party (if it is not already clear) whether the matter is urgent and likely to be of immediate personal concern to the student / staff member (e.g. a serious illness or the death of a family member or relative). In such cases it may be in order to provide such contact details, with appropriate safeguards (e.g. telephoning an identified person back at the given number rather than giving information in the course of the initial call).

- A third-party who contacts the College to make a complaint on behalf of a student/staff member should be informed that a complaint can be considered only when it is made (directly) by the student/staff member in question, except in the case of a vulnerable adult or person aged under 18 years old.
- Sensitive information such as financial or assessment data must never be given to a third-party without the explicit consent of the student/staff member ideally a phone call were the student can provide proof of identify.
- Any third-party who contacts the College, should be treated with courtesy, tact, sensitivity, diplomacy and patience at all times.

A data subject (see Appendix 2 for Glossary of Terms) is entitled to access his or her own personal data only. Students and staff are data subjects. The personal information of a data subject, including personal, assessment, attendance or financial must not be disclosed to a third-party, be they parent, potential employer, employer, professional body, sponsor, etc., without the consent of the individual concerned.

An agreement may be made to forward a communication to a data subject on behalf of a third-party, but no information should be disclosed about the data subject. In the case of research surveys where there is an agreement to forward documentation to data subjects, a notice should be included to the effect that no personal information has been released.

All information held by IBAT College Dublin about a student (e.g., name, address, date of birth, attendance or disciplinary record, examination results, academic progress, fees paid or due to the College) is confidential. This provision applies irrespective of the nature of system on which any information is held, manual or electronic.

Every data subject is entitled to confidentiality about his or her affairs regardless of his or her age (and of whether he or she has any disability).

There are ***five exceptions*** to this confidentiality:

1. In cases of certain emergencies (serious illness or death of a family member or relative). – as determined by the College Registrar or in their absence by a member of the Senior Management Group.
2. In cases where the student has given express permission in writing.
3. When, in accordance with legislation, student data is provided on a confidential basis to the Department of Social, Community and Family Affairs for the purpose of identifying possible abuses of the Social Welfare System.
4. When a written signed request is made by the Garda Síochana, section 8 (B) request under the Data Protection Act, 1988 whereby the data requested by Garda is required for the purposes of preventing, detecting or investigating offences, apprehending offenders in criminal proceedings..
5. Where relevant information has already been made public in a lawful manner and the College is requested to confirm it, e.g. provision of GN1B information to Garda.

Inappropriate disclosure of student data in response to contact from third parties can be a breach of the legislation. All mailings to students /staff are to be marked confidential and sealed. Students access examinations results on-line using their unique student number and password.

6. Securing Personal Data

IBAT College Dublin as the data controller must protect personal data from unauthorised access and must protected it from inadvertent destruction, amendment or corruption.

All IBAT College Dublin staff members are carefully coached and trained before being allowed to access confidential, personal or sensitive files.

The IT Team configures all network and mobile devices (whether desktop PC, laptop, smart phones, tablets, etc.) with the appropriate security standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.) to ensure the security and privacy of data within the organisation.

All wireless technologies/networks used to access the systems within IBAT College Dublin are encrypted to the strongest standard available.

Access to the IBAT College Server Rooms used to host hardware and software on which personal data is stored is restricted only to those staff members that have clearance to work there.

As well as physical access control the College's network administrators have added a level of security based on strict password and authentication polices combined with restricted access based on staff profiles and roles.

Network file and folder access for users is reviewed on a regular basis. Security access and privileges on the Student Management System (SMS) are continually monitored so IBAT College Dublin staff only have access to data which they require in order to perform their duties. There are regular reviews where privileges are increased or reduced if necessary, depending on the staff user's role.

IBAT College Dublin staff who transfer from one department to another, or resign, have their network privileges changed or removed accordingly including from any systems which allows access to or control of personal data.

All IBAT College Dublin computers are configured 'lock' when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys).

6.1 Anti-Virus

Anti-virus/Anti-spyware/Personal Firewall software is installed on all servers and computers in the College and is subjected to regular virus checks. In relation to downloading from the internet and e-mail attachments from unexpected sources caution needs to be exercised and unless the source is verified the action should not be conducted.

6.2 Firewalls

All IBAT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats.

6.3 Logs and Audit Trails

IBAT College Dublin has also introduced logging and reporting systems which are a valuable tool in assisting the network administrator in identifying abuses and developing appropriate responses. These systems are able to identify the user that has accessed a file, as well as the time of the access. A log of alterations made, along with author/editor is also available.

6.4 Remote Access

Where a staff member is allowed to access the network from a remote location (e.g. from home or from an off-site location), the following guidelines are implemented

- When accessing College data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place. The IT Team inform staff of such a link.
- Additional stringent security and access controls are in place – the mandatory use of strong passwords and security token authentication (i.e. two-factor authentication)
- IT Team ensures that only known machines (whether desktop PC, laptop, smart phones, Tablets, etc.) are configured appropriately to the required standards (e.g. with up-to- date anti-virus and anti-spyware software, full encryption, etc.) using strongest encryption methods available.

6.5 Wireless Networks

IBAT College Dublin wireless network use the latest devices, resulting in faster speed and security, data contamination on these devices is restricted with specific VLAN configurations.

6.6 Laptops/Smart Devices

Because Laptops, USB memory sticks, removable storage, smart phones, tablets and other form of portable computers are especially vulnerable – there is not only a higher risk of theft, but also a risk of accidental loss – a number of additional security measures are in place. Where a laptop is the personal property of an individual, the College has stipulated the conditions with such individuals under which data may be processed on personal computers.

- All portable devices must be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used.
- Passwords used on all devices are of sufficient strength to deter password cracking or guessing attacks.
- Personal, private, sensitive or confidential data is not stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption is employed regardless of the type of data stored.
- Data held on portable devices should be backed up regularly to the IBAT College Dublin servers.
- College owned portable devices must not contain unauthorised, unlicensed, or personally licensed software, all software must be authorised and procured through the IT Team.
- Anti-virus/anti-spyware/personal firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software.
- Laptops must be physically secured if left in the office overnight; when out of the office, the device should be kept secure at all times.
- Portable devices should never be left in an unattended vehicle.
- In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, the IT Team restricts the use of personal storage media and devices (e.g. floppy disks, CDs, DVDs, USB memory sticks, etc.)
- Only storage media provided by the IT department is permitted for use in College devices
- Staff owned devices such as portable media players (e.g. iPods, digital cameras, USB sticks, etc.) are restricted from connecting to College computers

6.7 Back-Up Systems

IBAT College Dublin has extensive backup systems which offer numerous recovery options from the loss or destruction of data. Backup of all network drives is performed on a daily basis with offsite storage to ensure that data can be recovered. Backup logs are checked on a daily basis to ensure the correct data backup has occurred.

The Student Management System (SMS) is backed up every night to another server, additionally the databases are also backed up within a historic archive on an external (off-site) backup device. Each daily backup is segregated into separate folders for each day of the month, then archived again for the last day of each month.

Both soft and hard copy of records of meeting minutes, committee and exam board meetings, external examiners reports, Broadsheets of results of cohorts of learners, copies of learner assessment scripts, etc. are maintained in accordance with the College Record Retention and Management Policy (reference **Appendix 1**), and are appropriately destroyed using a professional and accredited shedding company, aware of the sensitivity and their obligations for the treatment of such data in their possession.

6.8 CCTV at IBAT College Dublin

IBAT College Dublin has closed circuit television cameras (CCTV) located throughout both campuses covering buildings, internal space and pathways. This is necessary in order to protect against theft and for the security of staff, students and visitors.

Recognisable images captured by CCTV systems are considered “personal data”. They are, therefore, subject to the provisions of the Data Protection Acts.

Whilst CCTV footage is monitored by IBAT security staff, access to recorded material is strictly limited to authorised personnel, as identified by the College Director. The images captured are retained in accordance with the College Record Retention and Management Policy (reference **Attachment 1**). Exceptions to normal destruction policy may occur when the images identify a particular issue of interest, and are retained specifically in the context of an investigation of that issue.

CCTV footage may be entered as evidence in the event of disciplinary proceedings involving staff or students. CCTV footage is not disclosed to any third-party, except An Garda Síochána in the case of a disclosure pursuant to Section 8 (B) of the Data Protection Act 1998 (i.e. where it is

required for the purpose of preventing, detecting or investigating alleged offences) and any amendments to legislation thereafter.

There is signage, indicating that CCTV is in use, posted at the entrances to the campus.

A full list of camera locations is available on request from the College Data Protection Officer, who is the Registrar.

7. Privacy Statement

IBAT's privacy statement can be found on the IBAT website at www.ibati.ie and at **Appendix 2** of this policy.

8. Data Protection Personal Data Breach Code of Practice

Legislation imposes obligations on IBAT to process personal data that respects the rights of students and staff. The Data Protection Commissioner has approved a Personal Data Security Breach Code of Practice to help organisations react appropriately when they become aware of security breaches involving personal information. IBAT abides by this Code of Practice.

9. Responsibility

All IBAT staff members including, agents and contractors, who separately collect, control the content and use or process of personal data are individually responsible for compliance with legislation and this policy.

The Registrar will coordinate the provision of any support, advice or training required to ensure compliance with this policy. The Registrar will be assisted In certain instances by their colleague(s) in Finance,

IBAT College will conduct periodic audits (annual basis or when required) of its Data Protection procedures, in line with College internal audit processes. As part of the development of procedures for Data Protection Audit the following actions are recommended:

- Appoint a Compliance Officer (Auditor)
- Evaluate current practices and procedures to ensure that they meet the demands of the Acts
- Conduct a risk assessment by examining personnel files and evaluating the data (e.g. recruitment, disciplinary, leave of absence, health, finance)
- Examining all systems containing personal data
- Consider the location of any other data held
- Remove out of date and update inaccurate data
- Evaluate who has access to data
- Advise employees
    - How access is made available
    - Of the purpose for which data is held
    - To whom data may be disclosed
    - The source of data

The following table summarises the rules that apply.

"Opt-in" means you can only market an individual where you have their explicit consent to do so.

"Opt-out" means that you can market an individual provided you have given them the option not to receive such marketing and they have not availed of this option.

For an electronic communication to an Individual customer or business, an option to unsubscribe must be included.

	Postal Marketing	Text/Email Marketing	Phone Marketing to Landlines	Phone Marketing to Mobile Phones
Individual Customer (Important)	**Opt-Out**	**Opt-Out**	**Opt-Out**	**Opt-Out**
Individual Non-Customer	Opt-Out	Opt-In	Opt-In if on NDD, Opt-Out otherwise	Opt-In
Business Contacts (Customer & Non-Customer)	Opt-out	Opt-Out	Opt-In if on NDD, Opt-Out otherwise	Opt-In

9.1 All staff must ensure that:

- Personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform the College of any errors, corrections or changes, for example, change of address, marital status, etc.
- Personal data relating to living individuals which they hold, or process, is kept securely.
- Personal data relating to living individuals is not disclosed either orally, or in writing, accidentally or otherwise, to any unauthorised third-party.
- When supervising students who are processing personal data, that those students are aware of the Data Protection Rules, and IBAT College Dublin Data Protection Policy.

The following guidelines must be strictly adhered to when processing personal data contained in any administrative capacity:

- Staff must not disclose their password to any other member of staff or individual; all staff members who need access, including temporary staff, should use their own login.
- Staff must not disclose or discuss with any other member of staff or individual any personal data contained in any application, other than those members of staff who require the information for administrative/educational purposes.
- If it is deemed necessary to print personal data from an application, the data should be shredded once relevant work is complete.
- All IBAT College Dublin Staff should be careful in the use of the Personal Public Service Number (PPSN) in the Student Management System (SMS), on forms and documentation. There is a very strict statutory basis and code of practice when using PPSN. PPSN must only exist in the Student Management System (SMS) and should never be exported or used in other systems, the only exceptions are for QQI/UWTSD registration requirements.
- Staff PPSN data is retained by the College Accountant for payroll purposes and tax requirements.
- Printouts of sensitive reports can only happen within a designated functional area by authorised staff, for instance the Registry Assistant, Programme Administration Managers, Registrar, Head of School are the only ones who can access and print assessment data. This extremely important principle applies to other sensitive personal data such as HRM, Finance etc.
- Any reports produced from the Student Management System (SMS) must be shredded and disposed of in a safe and responsible manner, once relevant work is complete.

- If it is necessary to hold a printout from the Student Management System (SMS) for a period of time, it should be secured when not working with it and destroy by shredding once relevant work is complete.
- When working at one's desk, staff should make sure that screens displaying personal data are not visible to unauthorised persons, and should close applications and/or lock their workstation when leaving your desk, even temporarily.
- If it is necessary to export and save data from the Student Management System (SMS) in another application, such as Excel, the file should be deleted once relevant work is complete.
- Staff should not export files containing personal data onto their laptop or remove any personal data from the College.
- If a staff member is aware that a student has incorrect personal data or have been informed of a recent change then they should make the change, if an authorised data processor. If not authorised to make the change, then they should notify a staff member who can make any amendments.
- If there is a technical issue which prevents implementation of a change then the staff member should notify the IT Support team immediately at it.services@ibat.ie.

9.2 Responsibilities of Data Subjects

As IBAT holds personal data for students this makes each student a data subject under the legislation. This classification also applies to marketing leads, applicants, graduates and IBAT employees.

- All staff, students and other data subjects are entitled to be informed how to keep their personal data up to date
- All staff, students and other data subjects are responsible for;
  - checking that any information that they provide to the College is accurate and up to date
  - informing the College of any changes of information which they have provided, e.g. change of address, email address, telephone number, etc.
  - checking the information that the College sends out from time to time, giving details of information kept and processed
  - informing the College of any errors or changes (the College cannot be held responsible for any errors unless previously informed).

10. Marketing Guidelines

It's imperative that all student recruitment and marketing staff observe the strict obligations on the use of personal data for direct marketing.

The following are strict guidelines for processing personal data for direct marketing or student recruitment activities using electronic mail.

Almost all our direct marketing activities are to individual customers:

- Marketing leads from online enquiries and phone calls (implicit "Opt-In" from enquiry form and from caller)
- Applicants (Explicit and Implicit "Opt-In" in relation to invoice and payments)
- Student (Explicit "Opt-In" as a registered student)

All out bound marketing messages must include the unsubscribe link; the customer in this instance must have the right to object to receipt of further messages.

The only exception is if the customer gives you their consent to send such messages in the form of a marketing or financial pack to assist with their initial enquiry or processing a payment.

All batch marketing emails from the Student Management System (SMS) must include the unsubscribe link. This link is automatically added to the footer of all emails when using the "Marketing Mail Shot" facility in the Student Management System (SMS). All batch html newsletters and flyers must also use "Marketing Mail Shot" facility and adhere to the approved html template layout which includes the embedded unsubscribe link.

Once the customer uses the unsubscribe link it notifies the College via email and updates the customer status to unsubscribe. The customer will then be excluded from all further batch marketing emails and correspondence. Customer can also request by phone or email to be removed from direct marketing mailing lists, in this instance staff must manually set the customer status to unsubscribe. IBAT College Dublin Staff must never change the status from unsubscribe to subscribe unless they have obtained the explicit consent from the customer to do so.

All batch marketing emails must be filtered before they are sent to customer to ensure that the course we are marketing is similar to one the customer enquired about or was sold when the College obtained their contact details. Blanket batch emails are strictly forbidden; if a customer enquired about a business course then the marketing email must reflect this and complementary area(s) of study, and not contain courses which are solely based in another area of study. Also batch emails must only include customers where their initial online enquiry or completion of their course occurred within the last twelve months.

Batch marketing emails should never be sent using the "Admin Mailshot" facility as this service is for course admin and student support activities and as such ignores the unsubscribe status of the student, and excludes the unsubscribe footer in batch emails. Batch Text SMS direct marketing is expressly forbidden and must never be used for this purpose without the explicit consent of the customer. The only exception is if the SMS is to an individual customer supporting a sales or payment enquiry.

10.1. Direct Marketing

The basic rule that applies to direct marketing is that consent of the individual is needed to use their personal data for direct marketing purposes. As a minimum, an individual must be given a right to refuse such use of personal data both at the time the data is collected (an "opt-out" free of charge) and, in the case of direct marketing by electronic means, on every subsequent marketing message.

If any customer objects, the College may not use their personal data to market directly to them. The individual may withdraw their consent to direct marketing at any time. To ensure that the customer is excluded from any further direct marketing activities IBAT College Dublin also has an unsubscribe status against all customer records.

If the only reason for holding an individual's personal data is for direct marketing purposes, then the College must erase the personal data from any lists or databases that it holds once the individual has objected (requested that the College does so).

The only exception permitted in relation to the deletion of such records is if the customer seeking deletion is a registered student of the College and the deletion of this data would inhibit the on-going services and support to the student. The customer may also have assessment or financial data against their record, by law these records must be kept for a designated period and cannot be deleted. In this instance, the learner may be removed from the Marketing module within the SMS, and retained in the academic, financial, assessment modules, as appropriate.

10.2 Postal Marketing

Before the College can use personal data for postal marketing it must have first told the customers (or potential customers) that you intend to use their data for this purpose and give them an opportunity to refuse such use. Where the College has obtained the personal data from a third-party – including a source of information that is publicly available by law – the opportunity to refuse direct marketing material must be provided before any such material is sent.

10.3 Electronic Marketing

10.3.1 Phone (Everyone)

The making of marketing phone calls to the telephone number of an individual or business, other than a current customer who has given consent to the receipt of such calls, must be made in accordance with the regulations attached to the National Directory Database (the NDD).

The NDD also operates as a form of national telemarketing opt out register, which means that those persons wishing to contact subscribers by telephone for the purpose of direct marketing are obliged, under certain circumstances, to consult the NDD before making a marketing phone call to a mobile telephone number or an individual or business phone number.

The College operates in accordance with the regulations identified on the National Directory Database (the NDD) page of the Data Protection Commissioners website.

10.4 Electronic Mail

Electronic mail includes text messages (SMS), voice messages, sound messages, image messages, multimedia message (MMS) and email messages.

10.4.1 Individual and Business Customers

Where you have obtained contact details in the context of the sale of a product or service, you may only use these details for direct marketing by electronic mail if the following conditions are met:

(i) The product or service you are marketing is of a kind similar to that which you sold to the customer at the time you obtained their contact details.
(ii) At the time you collected the details, you gave the customer the opportunity to object, in an easy manner and without charge, to their use for marketing purposes.
(iii) Each time you send a marketing message, you give the customer the right to object to receipt of further messages.
(iv) The sale of the product or service occurred not more than twelve months prior to the sending of the electronic marketing communication or, where applicable, the contact details were used for the sending of an electronic marketing communication in that twelve month period.

NOTE: In relation to (iv) above, if the subscriber fails to unsubscribe using the cost free means provided to them they will be deemed to have remained opted-in to the receipt of such electronic mail for a twelve month period from the date of issue to them of the most recent marketing electronic mail.

10.4.2 Individuals ("Natural Persons") who are not Customers

If an individual is not a customer, you may not use electronic mail to send a marketing message to their contact address unless you have obtained the prior consent of that individual to the receipt of such messages – a consent that can be withdrawn at any time.

10.4.3 Business Contacts (Customers and non-Customers)

You may not use electronic mail to send a marketing message to a business contact address/number if the subscriber has notified you that they do not consent to the receipt of such communications.

11. Enforcement

This policy applies to all staff, agents and contractors of IBAT. In the event that there are changes in legislation this policy will be reviewed, updated and approved by the Board of Governors. This policy was approved by the BoG in March 2018.

If an individual believes their right to privacy or the protection of your personal data have been infringed, they have the right to bring a complaint to the Data Protection Commissioner at info@dataprotection.ie.

12 Further information

If you have any queries or require clarification on any aspect of these procedures and guidelines, please contact the College's Registrar at:

IBAT College Dublin, 16-19 Wellington Quay, Dublin 2, Ireland.
Email: dataprotection@ibat.ie

Tel: +353 (0) 1 8075055
Fax: +353 (0) 1 8075056

These guidelines are intended as a general introduction and are not an authoritative interpretation of the law. This Policy document will be reviewed regularly and updated as appropriate in line with any legislative or other relevant development.

Extensive information is available from the Data Protection Commissioner's website at www.dataprotection.ie or from the Office of the Data Protection Commissioner.

AP 1.10 Data Retention Schedule

The following are the retention periods for personal and non-personal data.

Data Type	Legal Requirement / Business Rationale	
ACADEMIC AFFAIRS		
Confidential learner records – examination entries, registration, Learner ECP and Deferral Requests, attendance.	2 years after completion of studies (provided no litigation is initiated during that period) *(Anonymised learner data may be retained for as long as required for administrative/statistical use, e.g.* name, address, date of birth, next of kin, places of employment, type of employment and where reported to Statistics provided/reported to Department of Education/HEA; QQI; UWTSD*)*	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
Meetings of - Programme Boards, School Management – minutes, membership, and relevant documentation	Permanent	
Quality Assurance policies, procedures and guideline documents - master copies and approval records	Permanent (Master, and e-version of superceded docs)	
(New) Programmes Submissions; Accreditation/(Re)Validation Reports; Approved Programme Document & Schedules, Programmes Approvals and Orders of Council, External Examiners reports, including college responses, Student Handbooks for each academic year, UWTSD (incl PTL reports)	Permanent	
Programme Feedback Learner (Individual) – Anonymised and explicit Other – lecturer / aggregate	Duration of studies* plus three years (provided no litigation is initiated during that period) Until relevant summary report is completed by Head of School and accepted by Programme Board	
Correspondence, documentation and reports from external bodies	5 years	

ADMISSIONS		
Enrolled learners - Direct & CAO application forms	Duration of studies* plus three years	Appraise and evaluate for archiving where relevant, otherwise confidential shredding/secure deletion of electronic records
Non-enrolled learners - Direct & CAO application forms	One year	
The following information is obtained, either online or directly from the prospective student at application stage and can be updated by members via the IBAT website Name, Date of Birth, Contact information Mobile number Email address Work phone number Post to home or work Work & Home details Address Phone number Payment is received via; Cheque; Cash, EFT Credit card payment details –are not held by IBAT. These go to Paypal, the credit card merchant provider. The credit card payment details are not held either electronically or in a manual file by IBAT.	Required the administration of services such as monitoring attendance on programmes. Details are required for the normal business operations.	Duration of studies and 5 years after graduation.

ASSESSMENT		
Copy of the continuous assessment brief and exam paper On the College Intranet	Permanent (5 years, or until module superseded by re-validation)	Appropriate filing/archive
Learner continuous assessment materials / exam script.	18 months, if not returned to learner (or shorter duration to be determined on an individual basis by the School if the physical size or resources tied-up makes 18 months retention impractical, but a minimum retention will be until one week after final date for lodging examination result recheck/review application) and provided no litigation is initiated during that period	Confidential shredding
Examination Results (individual and aggregate) – signed broadsheets (all awarding bodies) **Internal and** External Examination Board membership details, minutes and records	Permanent	Appropriate filing/archive
Learner examination records, registration and appeals documentation, including Turnitin or Vericite records.	Duration of studies* plus three years (provided no litigation is initiated during that period) *(Anonymised learner data may be retained for as long as required for administrative/statistical use)*	Appraise and evaluate for archiving where relevant, otherwise confidential shredding/secure deletion of electronic records

Finance Documentation		
All financial records are generally maintained for 6 years e.g. learner fee records, payroll, audit files, bank statements, refunds, capital projects, VAT / Tax returns, monthly cash flow reports, financial reports submitted to awarding bodies, expenses, purchase requisitions, funding of social activities, events, hardship funds etc.	6 Years	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
Exceptions are; Budget files and correspondence, financial policies, procedures and guidelines, legal documents, signed accounts & audits. Shorter durations apply for other activities, such as creditor records, purchase orders etc.	Permanent Various	Appropriate filing/archive
COMPANY DOCUMENTATION		
Governance – Academic Council, Board of Governors, Board of Directors and its sub-committees – Records of meetings, including agenda, approved minutes, supporting documentation, strategic plans	Permanent (e-copy)	Appropriate filing/archive
Company registration details, memorandum and articles of association, share-holding information, ownership documents	Permanent	
Risk Register (including risk assessment details)	Until updated/superceded	
Documents and correspondence relating to ***Litigation or Disputes*** which have been completed or settled.	3 Years, however (i) If the dispute or litigation were with a member of staff it will be destroyed 3 years after the member of staff ceases to be employed by the College. (ii) If the dispute or litigation were with a learner of the College, it will be destroyed 3 years after the learner ceased to be a registered learner of the College.	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records

Facilities		
College Health & Safety Records Including plans, drawings, accident report forms for learners and staff	Permanent	Appropriate filing/archive
Contractor's safety files	Permanent (legal requirement - 3 yrs after contract is complete) where is it kept	
Energy management files	3 years	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
Maintenance	For duration of machine's lifetime (provided no litigation is initiated during that period), particularly lifts.	
Human Resources		
Copy of advertisement, schedule of interviews, short-listing criteria and recruitment screening form	Retained for the duration of their appointment, unless litigation has been initiated during that period	Appraise and evaluate for archiving where relevant, otherwise confidential shredding/secure deletion of electronic records
Personnel records - employment history, qualifications, training, salary increments, appointment and termination details, medical certificates, leave of absence, birth certificates, staff development.	Duration of employment, plus 6 years *(Anonymised staff data may be retained for as long required for administrative/statistical use)*	
Pensions Arrangements - certificates of service, department returns, superannuation schemes, salary details, benefit statements	Permanent	
Documentation regarding ***Litigation*** or ***Dispute*** with a member of staff	3 years, after the member of staff has ceased to be such, and the dispute has been closed	
ICT SUPPORT		
Network account usernames, Web proxy logs and Internal staff details on email and telephone systems	Maintains record until individual leaves the College, and security copies for a further 3 months	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
LIBRARY		

Book stock (including electronic) records & borrowing records	Updated on an on-going basis	Confidential shredding
MARKETING		
***Printed Material* -** Prospectus, Learner Handbooks, Graduation Booklets	Permanent (2 hard copies, if/as appropriate)	Appraise and evaluate for archiving where relevant otherwise, confidential shredding/secure deletion of electronic records
CAREERS SERVICE		
Employer database – list of employers who contact the Careers Service with job opportunities for graduates	Updated on an on-going basis	Confidential shredding
First destination statistics of graduates	Permanent	Appropriate filing/archive

NOTES

* Duration of studies may be interpreted as learner's completion or discontinuance of/withdrawal from their programme of study (which includes completion of all assessment appeals periods.

Where Permanent retention is indicated, this is contingent on there being a business reason to do so e.g. all courses schedules are retained.

Breakdown of which departments manage and maintain general data

- Student College Application and Admissions Records Data – managed and maintained by the Student Recruitment Team, with electronic files and records stored within the Learner Management System (LMS).
- Student Disability Data – managed by the Registrars' Office, maintained by the Programme Administration Managers on hard copy student files, and electronic files and records stored within the LMS.
- Student Fees information - managed and maintained by the Admissions Team and College Accountant and electronic files and records within the LMS.
- Student Progression Data – managed and maintained by the Registrars' Office, Head of School, and Programme Administration Manager with electronic files and records stored within the LMS.
- Breach of discipline records – managed and maintained by the Registrars' Office.
- Examinable material – managed and maintained by the Registrars' Office and Programme Administration Managers with electronic files and records stored within the LMS.
- Examination records – managed and maintained by the Registrars' Office with electronic files and records stored within the LMS.
- College Finance data - managed and maintained by the College Director and College Accountant, with electronic files and records stored within the LMS.
- All Staff Records, including documentation pertaining to recruitment, job application, contracts, evaluation, discipline, and salary - managed and maintained by the College Director, Head of School, Registrar and functional managers.

AP1.11 IBAT College Dublin Access, Transfer and Progression Requirements

Quality & Qualifications Ireland (QQI) requires providers who submit programmes to them for validation for awards at Levels 6, 7, 8, and 9 (taught postgraduate), to develop access, transfer and progression criteria which are consistent with the procedures described in QQI's policy and criteria in relation to learners. Each favourably with existing (comparable) programmes in Ireland and beyond. Comparators should be as close as it is possible to find.

It is intended that this policy provides general criteria for admission, transfer and progression. Specific requirements in relation to individual programmes can be found in the submission application to QQI and will be published on IBAT College Dublin website when a programme has been validated.

Chapter 5 of the Quality Assurance Handbook details the admission procedures.

In general, a student's achievement at a specific Level on the NFQ prepares the student for undertaking a programme of study at the next Level. The entry requirements for admission to IBAT College Dublin programmes are also governed by several factors:

(i) A basic premise of minimum entry requirements is that applicants for programmes must 'have available statements of knowledge, skill and competence needed as a basis for successful participation'
(ii) There is comparability in the factors defined for similar programmes at a given Level on the NFQ offered by Higher Education Institute's at a given Level
(iii) There may be multiple access routes onto programmes at a given Level on the NFQ
(iv) The selection and admission of students is a competitive process as Higher Education institute's seek to ensure that students achieve the highest award performance levels on their programmes of study

The Recognition of Prior Learning policy and procedure covers access to programmes of non-standard applicants. The general minimum entry requirements are recommended by the Admissions Committee for consideration and approval by Academic Council. Programme Boards may seek additional entry requirements which must be approved by Academic Council. Irrespective of the access, transfer or progression routes, the decision to admit an applicant for a programme of study is made by the Registrar. The Admissions Committee has responsibility for reviewing admission standards and procedures, for considering the fairness and consistency of their application, and for overseeing the administration of the College's admissions system on behalf of the AC

Access Routes

Candidates for admissions to programmes run by IBAT College Dublin fall into the following admissions categories.

Direct Admissions

Candidates for entry to postgraduate programmes, add-on programmes, part-time and life-long learning programmes, corporate staff development programmes, and programmes run under initiatives such as Springboard apply directly to the College.

Candidates who wish to study English apply directly through the College.

Candidates from outside of Ireland apply directly to the College.

Indirect Admissions

Candidates for entry to the first year of all IBAT College Dublin full-time Higher Education (HE) programmes at Levels 6, 7 and 8 apply via the Central Applications Office (CAO).

Transfer routes

Candidates who are already registered on Higher Education programmes who wish to transfer to IBAT College Dublin programmes before they obtain an award should apply as follows:

- **Internal Candidates:** Candidates already registered on IBAT College Dublin programmes who wish to transfer to another IBAT College Dublin programme apply directly to the College.
- **External Candidates:** Candidates already registered on programmes in other Higher Education institutes who wish to transfer to IBAT College Dublin programmes apply directly to the College.

Progression Routes

IBAT College Dublin will notify students of potential progression routes for learners who have successfully completed programmes and obtained an award. Graduates should be aware that the decision to admit applicants is totally at the discretion of the receiving institution.

IBAT College Dublin Entry Requirements

Candidates must satisfy the minimum entry requirements and any additional requirements specified for their programme of choice to be considered eligible for entry.

Admission is based on the ranking of eligible candidates' overall award results where demand for places exceeds the number of places available.

Minimum Entry Requirements QQI Awards

The Academic Council establishes the minimum entry requirements for programmes to be submitted for validation to QQI on the advice of the Admissions Committee.

Additional entry requirements for programmes are determined by the Programme Boards in question and approved by Academic Council prior to submission to QQI.

When programmes are validated by QQI subject to conditions regarding admissions those conditions will apply for candidates entering the programme.

Ab-initio Programmes-Stage 1 entry

The general minimum entry requirements for entry on ab-initio programmes at NFQ Levels 6, 7 and 8 are stated in Table 1

Level 6, 7 and 8 Programmes-Advanced Entry

Normally a candidate seeking advanced entry into Stage 2 of a cognate Level 6, 7 or 8 must hold a cognate Level 6 QQI-FET major award.

Add-on Level 7 and 8 Programmes

Normally a candidate seeking entry onto a Level 7 add-on programme must hold a cognate Level 6 major award.

Normally a candidate seeking entry onto a Level 8 add-on programme must hold a cognate Level 7 major award.

Level 9 Programmes

Normally a candidate seeking entry onto a Level 9 taught programme must hold a cognate L8 major award with a minimum grade classification of H2.2 or equivalent.

Candidates who do not meet the H2.2 performance standard in a Level 8 award will be required to pass a qualifying assignment at a H2.2 performance standard as established by the Programme Board for the programme in question and as approved by the Registrar.

See below for specific entry requirements to the MBA awarded by UWTSD.

English Language Requirements

In addition to minimum entry requirements, non-native English speakers have an English language requirement.

EU and Non-EU, non-native English speakers who are applicants to Level 6, 7, 8 and 9 taught programmes are required to have a minimum score of 6.0 on the IELTS or equivalent. Refer to IBAT College Dublin English Language Recognised Equivalence AP1.3a.

Major Award Level	Leaving Certificate	QQI-FET
Level 6 and 7	Grade O6/H7 in 5 Leaving Certificate subjects including English and Mathematics.	Any QQI-FET/FETAC Level 5/6 award
Level 8	Grade O6/H7 or better in 6 Leaving Certificate subjects including English and Mathematics, two of which must be passed in higher level papers at Grade H5 or higher	Any QQI-FET/FETAC Level 5/6 award in a cognate discipline including a distinction grade in at least 3 components.
Level 9 (Taught)	Cognate Level 8 major award with a minimum grade classification of H2.2 or equivalent.	

Table 1 Minimum Entry Requirements

Leaving Certificate Examination Sittings

Points will be calculated on the basis of the six best subjects in one Leaving Certificate sitting only. Eligibility requirements, in terms of Leaving Certificate subjects, may be satisfied over two or more Leaving Certificate sittings.

Bonus Points for Mathematics awarded

A bonus of 25 points will be allocated to students who achieve a grade H6 or above in Higher Level Mathematics. This means that the maximum cumulative Leaving Certificate points will increase from 600 to 625 (existing points plus bonus points).

Foundation Level Mathematics.

A pass in Foundation Level Mathematics at F2 or higher will be considered as meeting the minimum entry requirements for courses which require a minimum entry level H7/O6 in Ordinary Leaving Certificate Mathematics.
Students with Foundation Level Mathematics at F2 level or higher must have passed four other subjects with a minimum grade of H7/O6 for the Higher Certificate (Level 6) and Bachelor Degree (Level 7) Programmes.
Foundation Level Mathematics may be used for the purpose of determining Leaving Certificate points and where it is so used the following scale will apply:

F1	F2
20	12

Leaving Certificate Applied (LCA)

The Leaving Certificate Applied does not meet the minimum entry requirements to IBAT College Dublin programmes. Holders of the LCA may gain entry through the QQI-FET/FETAC Level 5 or Level 6 awards scheme.

Entry Requirements

Admissions Criteria MBA

Abstract from:

IBAT College Dublin - PROGRAMME VALIDATION DOCUMENT - 27 August 2013

Master of Business Administration

Including exit awards of:

- Postgraduate Certificate in Business Administration
- Postgraduate Diploma in Business Administration

Selection Procedure

IBAT College Dublin will adhere to the procedures outlined in the relevant sections of the UWTSD Academic Quality Handbook (Collaborative Learning and International Programmes).

Applicants are requested to complete an application form and provide references from two academic or industry related referees. Applicants will normally be interviewed on the basis of entry requirements and references.

Entry Requirements

Admission requirements will be consistent with IBAT College Dublin's admissions policy and the entry requirements of the individual programme as outlined in the individual programme specification.

All applicants will be individually considered for admission using the following criteria:

- A minimum of a 2:2 honours degree, or an appropriate equivalent, i.e. a professional qualification from a recognised education Institution in Ireland or abroad.
- Appropriate period of prior experiential learning and/or relevant experience in management or business related employment fields, or a related area/discipline/subject experience. This is normally equivalent to, or comparable with, at least two years relevant experiential learning. This period is not prescriptive and will be interpreted flexibly as a part of consideration for entry.
- The applicant's ability to complete the programme satisfactorily and benefit from it.
- Applicants who do not fully satisfy the general criteria will be considered and may be admitted if they are able to demonstrate that they are capable of successfully undertaking and completing the programme at the required standard and are able to contribute fully to, and benefit from, the learning experiences delivered within the programme.
- Applicants who have been taught and assessed in languages other than English should have an English language equivalent to IELTS 6.0.

Admission criteria and entry qualifications for the MBA Programme will also include the applicant having:-

i. A non-honours Bachelors degree in a business related or cognate subject and relevant evidenced experience (normally equivalent to or comparable with two years)
ii. An honours degree in a non-business related or cognate subject where the applicant has evidenced relevant experience (normally equivalent to or comparable with two years)
iii. An equivalent certificated degree from an oversees institution to those specified in (i) and (ii) above
iv. Non-degree qualifications such as the Higher National Diploma in Business related subjects (e.g. EdExel), or equivalent overseas qualifications, where the applicant has appropriate employment experience (normally equivalent to or comparable with a minimum of three years)
v. Qualifications from relevant Professional Bodies, which are at a level below UK honours degree and relevant professional experience,(normally equivalent to or comparable with a minimum of three years)

Other potential candidates

Candidates with significant management, business, related employment fields or related area/discipline/subject experience or similar related employment field experience may be admitted onto the programme without a degree qualification (or degree equivalent) if they can demonstrate their potential to meet the learning requirements of the programme.

Eligibility will be determined by means of an interview with the admissions officer and subject to academic signoff by the MBA Programme Director. All potential applicants will be required to provide written references for their work experience.

Applicants may also be formally considered for admission to the programme using the appropriate APEL/RPL as outlined in the IBAT College Dublin Recognition of Prior Learning Policy.

Advanced Entry onto the Programme

Entrants with relevant and acceptable professional accreditation may be considered for exemptions. For example, applicants with CIPD accreditation may be exempt from the following modules: Human Resource Management or Strategic Management. Entrants with ACCA accreditation may be considered for exemptions from certain relevant modules and entrants with CIM and CMI accreditation may also be considered for advanced entry or exemptions.

Interviews

The College believes that the interview is an important tool in assessing the suitability of applicants and normally all applicants will be interviewed. If a face-to-face interview is not possible then a telephone interview will be held. In certain circumstances an offer of a place may

be made based on the application form alone including academic history, a personal statement and appropriate reference(s).

English Language requirements for International Students

International students, for whom English is not a first language, are subject to additional requirements and will be requested to provide evidence of proficiency of spoken and written English to meet the demands of the MBA Programme. A IELTs score of 6.0 or TOEFL 575 or an equivalent must be obtained.

AP 1.12 Guidelines on Assessing Group Work

1 Policy

This guideline supports the IBAT assessment policies as contained in the IBAT Quality Assurance Handbook 2018 (V4.3) and the IBAT Assessment Strategy (Associated Policy 1.5).

The overarching policy is that every learner has the opportunity to demonstrate that they have achieved the learning outcomes for a module and programme as laid out in the IBAT Assessment policy particularly:

- learners have the opportunity to demonstrate their learning achievement
- assessment opportunities support standards based on learning outcomes

Adapted from QQI Assessment and Standards 2013

Where group work is used each learner will receive an individual grade for a group assignment.

Where group work is to be reassessed or where there is a valid reason for an alternative assessment the module learning outcomes must be reviewed. If group work or team work is a learning outcome then any alternative assessment or reassessment task must be designed to measure that learning outcome. Where group or team work is not a learning outcome then an alternative assessment may be substituted subject to the programme and college regulations.

2 Procedure

The individual grade for group work is weighted between a grade for the group assignment itself (***product***), which will be the same for all members of the group and a grade for each individual learner's contribution to that assignment and their contribution to the team (***process***).

There are various strategies used to agree the weighting between product and process and these are agreed for each module by the programme team. A number of examples of how this works are provided below.

Group membership may be either prescribed by the Module Leader or allowed self-select as deemed appropriate.

The assessment of group work provides an opportunity for self and peer assessment. Where these are used it is under the close supervision and moderation of the assessor and should not contribute to a significant element of the mark. The module leader is responsible for the validity of peer assessment and must be able to provide evidence, such as a rubric as in Example 1 below, to share with the External Examiners or in the case of an appeal.

It is highly recommended that the group test the work using similarity software prior to submission and resolve any issues that this may raise before submission.

Where the assessor alleges plagiarism in a piece of group work the group must supply details of their individual contribution and any evidence of meetings and any communications relating to the allocation of workload. All members of the group should ensure that the joint contribution did not benefit from academic misconduct.

Example 1:

A group project is worth 30% of a module.

The module leader has agreed that the marks for the assignment will be split evenly between a group contribution and the individuals' contribution to the assignment. The group work is assessed through marking the group presentation/ slides and associated documentation. The individual contribution is assessed by each member of the group completing a rubric determined by the module leader detailing and grading the contribution of each team member to the project.

The module leader has agreed that the individuals' contribution to this assignment is to be measured by assessing the individuals' participation in the group presentation and individuals' ability to answer questions on the presentation.

Each student in the group will get a grade for the assignment which will be identical and will contribute to 50% of the overall group assignment grade. In addition each student will also receive a personal grade established by how well they contributed to the project which will be peer assessed. The marks will be combined to give an overall, yet individual, grade for the group assignment reflecting the student's achievement of the module learning outcomes.

Example 2:

A group assignment is worth 50% of the total marks for a module. As above the product and process were weighted evenly.

In this case the module leader has agreed that the individuals' contribution to this assignment is to be measured by assessing the individuals' participation in the group project through the marking of a self-evaluation report which is to be submitted by EACH individual student at the same time as the group project is submitted. This self-evaluation report documents the work carried out by the individual (self-assessment) in relation to the group project and to highlight their learning over the duration of the project and to highlight what they would do differently.

Each candidate will receive the same mark for the assignment but in the case of one learner the log was not submitted. Even if the group assignment was graded at 70% the candidate that did not submit the log or contribution report would fail that element of the module. This illustrates the importance of participation in the team process and evidencing that participation.

Contingency Plan for On-Line Delivery and Assessment

Bachelor of Arts (Hons) in Business
three-year, ab initio, 180 ECTS

Valid from 13th March 2020 to end of College Closure

IBAT College Dublin
16-19 Wellington Quay
Temple Bar
Dublin 2

Summary

Following the announcement from An Taoiseach on the 12th March 2020 and the updates provided by the Department of Education and Skills that Higher Education Institutions will remain closed to students until 19 April 2020, IBAT College has transitioned to delivering all academic material remotely. This includes the undergraduate programme awarded by QQI, post-graduate programme awarded by UWTSD, English Language programmes and Professional Diplomas.

The approach at IBAT is to facilitate remote learning in virtual classrooms supported by the IBAT Virtual Learning Environment - Moodle.

Our priority is to provide ongoing delivery and support to learners whilst preserving the academic standards and integrity of all programmes.

This document describes the delivery and assessment of the BA (Hons) in Business awarded by QQI for the rest of this semester.

IBAT currently have learners at Stage 1 in both Semesters 1 and 2 of the programme. Whilst this is not the award stage, there is an exit award of Certificate in Arts in Business after successful completion of Stage 1.

Contingency Strategy

Phase 1 Suspension of Classes

On announcement of the closure the College closed to all students from the 13th March. Face to face classes were suspended until the 30th March to give the staff sufficient time to transfer to remote delivery following an orderly process. English Language transitioned on the 19th of March followed by Professional Diplomas and Higher Education on the week commencing the 30th March. A Reading Week was scheduled in this period so the suspension has pushed the academic calendar out by one week. These revised dates impact on the dates of the Exam Boards but not on the commencement of the next semester.

A revised Academic Calendar is included in Appendix 1.

Phase 2 Virtual Delivery

The IBAT online approach will be synchronous virtual-class room delivery. These classes will adhere to the current timetable. Where developmental workshops had been scheduled these will be managed virtually either through asynchronous approach such as video or simply by producing a Power-point deck – this will depend on the nature of the workshop.

To ensure continuity Moodle will continue to be used as the repository of all shared material and all interaction will be through Google Classrooms supplemented by Google Hangouts.

Staff have been trained via online workshops using Google Classrooms and all staff have confirmed that they have the equipment required. See Table 5 for the list of the current lecturers.

There are 13 students at Stage 1 Semester 2 and 16 students at stage 1 Semester 1 on the BA (Hons) in Business. All learners have confirmed that they have access to a laptop or other suitable device.

Virtual classes commenced on Tuesday 31st of March.

Phase 3 Revised Assessment Strategy

This document is the QA record for the revised assessment strategy. The revised strategy applies only to the period of closure mandated as a result of the current global pandemic. Support for learners whilst maintaining the integrity of the award are the primary concerns.

This approach was informed by the 'Guiding Principles for Alternative Assessments' (Devised in response to the covid-19 emergency restrictions) - QQI 26 March 2020

The programme has learners at Stage 1 in both Semesters 1 and 2. Therefore the focus is in assessment for progression within a programme.

When revising the assessment strategy the Stage 1 Minimum Intended Stage Learning Outcomes were consulted. There has been no change to any learning outcomes.

The programme assessment strategy also includes the assessment of embedded skills and competencies see Tables 3 and 4.

IBAT do not have the facilities or expertise to manage the normal traditional examinations on-line with full confidence that academic integrity can be guaranteed. Therefore, a revised assessment strategy has been prepared to ensure that learners are provided with appropriate opportunities to demonstrate they have achieved the module and stage learning outcomes.

The approach has been systematic and followed a process:

1. Assessment instruments were reviewed for each module.
2. Examinations and In-Class Tests were replaced by alternative instruments.
3. Where a change to assessment was required (10 of 12 modules) a proposed revised assessment strategy was prepared by the lecturer, guided by the School and reviewed by the External Examiner.
4. The revised assessment instruments were constructively aligned to the MIMLO's.
5. The assessment of skills and competencies was reviewed against Table 3 below.
6. Academic integrity was an important consideration in the design of alternative assessment instruments.
7. The External Examiner was part of process and consulted throughout.

The revised Stage 1 assessment strategy was approved by the External Examiner on the 29th March and this paper was approved by the Academic Council by circulation on 3rd of April.

Revisions to Modules

Two modules required no changes and a further two modules required no substantive change, however the challenges of managing a group presentation online and in the

prevailing environment is acknowledged and further learner support has been agreed as this assessment is administered.

Where there was either a written examination or an in-class test, these were substituted by one or more of the following:

- Online MCQ Test in real time
- Online Short Answer Test in real time
- Open Book Work Sheet comprising worked calculations.
- Open Book Work Sheet- A series of long answer questions
- Written Assignments

Where a written assessment was substituted as an alternative to a written examination, the word count of the substituted assessment was appropriately aligned with the learner effort required.

Submission dates have been realigned and the study and exam weeks are used to ensure there is adequate time to undertake summative written assignments or work sheets.

All revised assessment instruments are subject to the approval of the External Examiner.

Table 1 – Summary of changes

Module	**Replacement Instrument**	**% Weighting**
1.01 Business Maths	Online MCQ Test in real time*	20%
1.01	Open Book Work Sheet comprising worked calculations.	40%
1.03 Introduction to Business	Open Book Work Sheet- A series of long answer questions requiring detailed answers to be arranged at the end of the module circa 2000 words	60%
1.05 Marketing Fundamentals	Online Short Answer Test in real time*	25%
1.05	Open Book Work Sheet – A series of long answer questions – 1500 words.	35%
Sem 2		
1.07 Financial Accounting	An assignment covering theoretical concepts 2500 words	50%
1.07	Open Book Work Sheet- A series of long practical problems	50%
1.08 Microeconomics	Online Short Answer Test in real time*	40%
1.08	Open Book Work Sheet- A series of long answer questions requiring detailed answers to be arranged at the end of the module circa 2000 words.	60%
1.09	Online Short Answer Test in real time*	40%

Macroeconomics		
1.09	Open Book Work Sheet- A series of long answer questions requiring detailed answers to be arranged at the end of the module circa 2000 words.	60%
1.11 Principles of Business Law	Written Assignment – Formative (2000 words)	40%
1.11	Written Assignment – Summative (2500 words) with short viva	60%
1.12 Statistics	A summative assignment based on data presentation, graphical skills and problem solving – to include worksheets and graphs.	50%

*Instruments requiring assurance of academic integrity.

Assuring Academic Integrity

Four assessment instruments across the first stage were not designed as open book tests.

In semester 1 – there are two tests are worth 20% and 25% respectively and are designed to test knowledge appropriate to Stage 1 at level 6. One is a multi-choice test and one is a series of short answer questions. These will be held in class time with the lecturer present.

In semester 2 – there are two tests worth 40% each and designed to test knowledge and reasoning appropriate to Stage 1 at level 6. Both are a series of short answer questions. These will be held in class time with the lecturer present but will be held over a longer time period.

Over this period the College will take two approaches to assuring academic integrity.

- An integrity pledge
- An integrity test

Integrity Pledge

All leaners will be required to sign an integrity pledge adapted from UC San Diego Academic Integrity Office from a link recommended by QQI. This highlights the importance of academic integrity to leaners and is based on trust. It puts the onus of academic integrity on the student and treats them as significant and valued stakeholders in the assessment process.

Integrity Test

In the case of the larger volume tests in semester 2, the test will be followed up by the lecturer asking the students in breakout rooms to develop one answer in more detail in the form of a short question and answer session. This is manageable with the low numbers enrolled on the programme.

The lessons learned from this will inform the further development of the student code of conduct as it relates to Academic Integrity.

Learner Supports

Programme Administration Manager

The Programme Administration Manager is in regular communication with students *via* email and providing the usual supports.

Library Services

Each Indicative Bibliography was reviewed by the lecturer to update it and ensure there are adequate online services for those who no longer have access to the physical collection. The ICLA have also extended our license and given us guidance on what we can share with our students in the virtual classrooms and on our VLE (Moodle) and remain within our copyright licence. The librarian is contactable via the online chat in addition to normal channels.

Counselling

The Students Affairs Co-ordinator is also available to the students online and manages the counselling service which has also moved online. This is recommended by all accredited counselling bodies for safety reasons and the supervisory counsellor has been notified of, and supports the online service.

The Programme

Programme Management

There will be no change to programme management as it is intended to manage the Programme Board and the Class Representative Meeting in virtual classrooms.

The programme questionnaire will change to account for the altered delivery mechanism and ensure sufficient learner feedback is obtained.

The progress of remote delivery and assessment will be monitored by the Head of School and Registrar and further supports put in place as required.

Minimum intended programme learning outcomes (MIPLOs)

The minimum intended programme learning outcomes (MIPLOs) for this proposed **BACHELOR OF ARTS (HONOURS) IN BUSINESS - NFQ, Level 8** have been expressed in terms of knowledge, skill and competence.

On successful completion of this proposed **BACHELOR OF ARTS (HONOURS) IN BUSINESS - NFQ, Level 8** programme the learner will be able to:

Knowledge – Breadth	**MIPLO-01**	Demonstrate an extensive knowledge and in-depth understanding of current theories, concepts and principles of key business discipline such as management and strategy, economics, marketing, finance, HR and ICT and entrepreneurship in both domestic and international business environments and how the application of modern technologies such as data analytics and current communication systems enhance the field.
Knowledge – Kind	**MIPLO-02**	Evaluate concepts and theories of the core subfields of business including management and strategy, economics, marketing, finance, HR, ICT and entrepreneurship and be able to apply them creatively to develop business opportunities.
Skill – Range	**MIPLO-03**	Critically review and analyse a diverse range of business data, select appropriate methodological techniques to solve business problems and present, defend and advocate insights and ideas.
Skill – Selectivity	**MIPLO-04**	Demonstrate a range of professional attributes, judgement and informed analytical skills to analyse problems and apply creativity in designing and implementing solutions and effectively communicate responses in a modern, global business environment
Competence – Context	**MIPLO-05**	Contribute to the process of business development, using knowledge from a range of subject areas, analyse information to contribute to solutions to complex business problems, accept accountability and have a critical understanding of ethical implications in business and the wider social context.
Competence – Role	**MIPLO-06**	Demonstrate the ability to work collaboratively as a member of a team in interdisciplinary and multicultural environments and exercise autonomy, self-direction and initiative as a team leader in dynamic and complex business situations.
Competence – Learning to Learn	**MIPLO-07**	Demonstrate a self-awareness and ability to initiate own professional development and the development of others, through coaching and mentoring to function effectively and ethically in complex business environments. Be amenable to engaging with new developments and practices within Business.
Competence – Insight	**MIPLO-08**	Articulate the wider social, political and business contexts within which the business professional operates and the need for high ethical, professional and legal standards in one's work and in particular towards stakeholders and society at large.

Minimum Intended Stage Learning Outcomes after Stage 1

The Minimum Intended Learning outcomes for **Stage 1.**

On successful completion of stage 1 of this proposed programme the learner will be able to:

Knowledge – Breadth	**MISLO-1.1**	Demonstrate a basic general knowledge of a wide variety of industry and business types, sources of business information, the economic context in which business operates, and an understanding of the challenges, skills and techniques involved in business.
Knowledge – Kind	**MISLO-1.2**	Recognise general established business disciplines, management, economics, marketing, finance and ICT, and the connectivity between them in order to understand general business situations.
Skill – Range	**MISLO-1.3**	Apply a broad range of business skills to present business problems, and communicate possible solutions, effectively in a work situation.
Skill – Selectivity	**MISLO-1.4**	Collect and present data to facilitate solutions to well defined business problems. To contribute to decision making in response to qualitative and quantitative data, and apply general solutions to well-defined problems.
Competence – Context	**MISLO-1.5**	Apply a range of skills in a variety of structured business contexts, exercise discernment in applying such skills and knowledge, identify solutions to well defined problems and present the information in written and oral form.
Competence – Role	**MISLO-1.6**	Contribute effectively, both autonomously and as a member of a team, to work ethically and professionally with the capacity for creativity and innovation.
Competence – Learning to Learn	**MISLO-1.7**	Reflect on and take responsibility for own learning and to have the ability to adapt to cultural and educational contexts; demonstrating, where appropriate, effective interpersonal, social and communication skills.
Competence – Insight	**MISLO-1.8**	Participate in structured business activities, with a clear sense of purpose, in a confident, motivated and responsible manner, whilst showing respect for others, the environment and the law.

The College's Learner Recruitment department provides administrative assistance and advice to international applicants, for example, in respect of visa processing.

Outline of the curriculum

Table 2:

STAGE 1: Semester 1	**Status**	**ECTS**	**STAGE 1: Semester 2**	**Status**	**ECTS**
Business Mathematics	M	5	Statistics	M	5
ICT in Business	M	5	Financial Accounting	M	5
Introduction to Business	M	5	Microeconomics	M	5
Learning and Development	M	5	Macroeconomics	M	5
Marketing Fundamentals	M	5	Management Principles	M	5
Effective Communications for Business	M	5	Principles of Business Law	M	5

Skills and Competencies

Table 3: Skills and Competencies groups aligned to MIPLOs

SKILLS AND COMPETENCIES GROUPS	MIPLO
Business Knowledge and Knowhow S1 · Applying subject understanding: use of disciplinary understanding from the HE programme. · Commercial awareness: operating with an understanding of business issues and priorities.	MIPLO1 MIPLO5
Communication S2 · Written communication: clear reports, letters etc. written specifically for the reader. · Oral presentations: clear and confident presentation of information to a group · Influencing: convincing others of the validity of one's point of view · Negotiation:	MIPLO4
Self-Management and Setting Goals S3 · Self-management: ability to work in an efficient and structured manner. · Self-awareness: awareness of own strengths and weaknesses, aims and values. · Prioritising: ability to rank tasks according to importance. · Planning: setting of achievable goals and structuring action.	MIPLO6 MIPLO7
ICT Skills S4 · Computer literacy: ability to use a range of software.	MIPLO1
Problem Solving / Research S5 · Critical analysis: ability to 'deconstruct' a problem or situation. · Problem solving: selection and use of appropriate methods to find solutions. · Decision making: choice of the best option from a range of alternatives. · Creativity: ability to be original or inventive and to apply lateral thinking.	MIPLO2 MIPLO3 MIPLO4
Teamwork and Cultural Awareness S6 · Global awareness: in terms of both cultures and economics. · Ability to work cross-culturally: both within and beyond national boundaries. · Political sensitivity: appreciates how organisations actually work and acts accordingly. · Team work: can work constructively with others on a common task.	MIPLO6 MIPLO8
Independent Self-Starter S7 · Independence: ability to work without supervision. · Initiative: ability to take action unprompted.	MIPLO7
Ethics S8 · Acting morally: has a moral code and acts accordingly. · Ethical sensitivity: appreciates ethical aspects of employment and acts accordingly.	MIPLO5 MIPLO8

Table 4: Modules where skills are embedded – examples.

	STAGE 1	
1.01	Business Mathematics	S2, S4, S5
1.02	ICT in Business	S1, S4
1.03	Introduction to Business	S1, S2
1.04	Learning and Development	S3, S7, S8, S9
1.05	Marketing Fundamentals	S1, S8

1.06	Effective Communications for Business	S2, S3, S6, S7
1.07	Financial Accounting	S1, S2
1.08	Microeconomics	S2, S5
1.09	Macroeconomics	S2, S4,S5
1.10	Management Principles	S2, S3, S7
1.11	Principles of Business Law	S1, S2, S8
1.12	Statistics	S2, S4, S5

Complement of staff

Updated for implementation Phase:

The programme management team comprise:

Joe Gorey	College Principal
Dr Finbarr Murphy	Registrar
Dr Brid Lane	Head of School
Emmalyne Smith	Programme Administration Manager

Table 5 Academic staff currently assigned to this proposed programme

MODULE TITLE	Status	Level	ECTS	Module Lecturer
STAGE 1				
Business Mathematics	M	6	5	Jennifer McCarthy
ICT in Business	M	6	5	Kevin O'Shaughnessy
Introduction to Business	M	6	5	Lynette Roe
Learning and Development	M	6	5	Morgan McKnight
Marketing Fundamentals	M	6	5	Colm Dunne
Effective Communications for Business	M	6	5	Colm Dunne
Financial Accounting	M	6	5	Michael Ellis
Microeconomics	M	6	5	Stephen Walsh
Macroeconomics	M	6	5	Stephen Walsh
Management Principles	M	6	5	Lynnette Roe
Principles of Business Law	M	6	5	Niall Fahy
Statistics	M	6	5	Jennifer McCarthy

Proposed Programme Schedule

Proposed Programme Schedule: BA (Hons) - Stage 1, Full-time

Name of Provider:	IBAT College Dublin
Programme Title	Bachelor of Arts (Honours) in Business
Award Title	Bachelor of Arts (Honours)
Stage Exit Award Title[3]	Certificate in Arts in Business
Modes of Delivery (FT/PT):	Full Time
Teaching and learning modalities	Lectures; Tutorials; Guest Lectures; Case Studies; Practicals; Blended e-learning; Group Work; Research; Information Literacy Classes; Reflection; Support Classes

Award Class[4]	**Award NFQ level**	**Award EQF Level**	**Stage** (1, 2, 3, 4, …, or Award Stage)**:**	**Stage NFQ Level[2]**	**Stage EQF Level[2]**	**Stage Credit (ECTS)**	**Date Effective**	**ISCED Subject code**
Major	8	6	Stage 1	6	5	60	03/2019	0413

Module Title (Up to 70 characters including spaces)	**Semester no where applicable. (Semester 1 or Semester2)**	**Module**		**Credit Number**	**Total Student Effort Module (hours)**					**Allocation Of Marks (from the module assessment strategy)**			
		Status	**NFQ Level[1] where specified**	**Credit Units** / **ECTS Credits**	**Total Hours**	**Class (or equiv) Contact**	**Directed e-learning**	**Hours of Independent**	**Work-based learning**	**C.A. %**	**Supervised Project %**	**Proctored practical demonstration %**	**Proctored written exam %**
Business Mathematics	1	M	6	5	125	36	-	89	-	100	-	-	-
ICT in Business	1	M	6	5	125	36	-	89	-	100	-	-	-
Introduction to Business	1	M	6	5	125	36	-	89	-	40	-	-	60
Learning and Development	1	M	6	5	125	36	-	89	-	50	50	-	-
Marketing Fundamentals	1	M	6	5	125	36	-	89	-	-	40	-	60
Effective Communications for Business	1	M	6	5	125	36	30	59	-	100	-	-	-
Financial Accounting	2	M	6	5	125	36	-	89	-	40	-	-	60
Microeconomics	2	M	6	5	125	36	-	89	-	40	-	-	60
Macroeconomics	2	M	6	5	125	36	-	89	-	40	-	-	60
Management Principles	2	M	6	5	125	36	-	89	-	-	100	-	-
Principles of Business Law	2	M	6	5	125	36	-	89	-	40	-	-	60
Statistics	2	M	6	5	125	36	-	89	-	100	-	-	-
Special Regulations (Up to 280 characters)													

Appendix 1 Revised Academic Calendar

Covid Contingency
Revised Academic Calendar

February 2020 Intake			**October 2019 Intake**	
TW1	17/02/2020	Sem 2 Ex	TW1	17/02/2020
TW2	24/02/2020	Boards	TW2	24/02/2020
TW3	02/03/2020		TW3	02/03/2020
TW4	09/03/2020		TW4	09/03/2020
Suspended	16/03/2020		Suspended	16/03/2020
Suspended	23/03/2020		Suspended	23/03/2020
TW5	30/03/2020		TW5	30/03/2020
TW6	06/04/2020		TW6	06/04/2020
TW7	13/04/2020		TW7	13/04/2020
TW8	20/04/2020		TW8	20/04/2020
TW9	27/04/2020		TW9	27/04/2020
TW10	04/05/2020		TW10	04/05/2020
TW11	11/05/2020		TW11	11/05/2020
TW12	18/05/2020		TW12	18/05/2020
SW1	25/05/2020		SW1	25/05/2020
EXW1	01/06/2020		EXW1	01/06/2020
MKW1	08/06/2020		MKW1	08/06/2020
MKW2	15/06/2020		MKW2	15/06/2020
Pre Board	22/06/2020		**Pre Board**	22/06/2020
Exam			**Exam**	
Board	29/06/2020		**Board**	29/06/2020
Hols	06/07/2020		ISB	06/07/2020
Hols	13/07/2020		ISB	13/07/2020
Hols	20/07/2020		ISB	20/07/2020
Hols	27/07/2020		ISB	27/07/2020
Hols	03/08/2020		ISB	03/08/2020
Hols	10/08/2020		REXW1	10/08/2020
Hols	17/08/2020		MKW1	17/08/2020
Hols	24/08/2020		MKW2	24/08/2020
Sem 2	31/08/2020		Ex Boards	31/08/2020
			Hol	07/09/2020
			Stage 2	14/09/2020

AP1.14 Policy on Recording of Oral or Visual Presentations

Introduction

IBAT College Dublin is committed to the privacy of all staff and learners, providing equal opportunities for all staff and learners and is fully committed to the principles in The Equal Status Acts 2000-2018 ('the Acts') prohibiting discrimination in the provision of goods and services, accommodation and education.

This policy on the Recording of Oral or Visual Presentations applies to all programmes.

What is an oral or visual presentation?

An oral or visual presentation includes lectures, seminars, tutorials, laboratories, practical exercises, and/or field trips.

There are various reasons for a lecture or visual presentation to be recorded:

1. A learner may request to record a presentation for their own study often under the IBAT Reasonable Accommodation Policy (QAH, Section 8.8)

2. The College or a lecturer may wish to record a visual presentation for inclusion on the VLE for study purposes

3. A presentation may be recorded for assessment purposes

1. Learner requests to record an oral or visual presentation

A learner with specific needs may apply for Reasonable Accommodation. Their request is made to and assessed by the Office of the Registrar. This policy should be read in conjunction with the College's Reasonable Accommodation Policy, Section 8.8 in the College Quality Assurance Handbook.

Where the outcome of that assessment is that the learner would benefit from being able to record oral or visual presentations or receive the recording of online delivered lectures the learner will be authorised to do so. An authorised learner will be allowed to record such presentations on the following conditions:

- The intellectual property remains with the college
- The recording is for the learners own educational use and is not reproduced or distributed to any third party. The only exception is where a scribe is used to transcribe the recording for the sole use of the learner.
- The learner must attend classes, recording presentations is not a substitute for attendance and the authorisation to record may be revoked if the learner is deemed to be misusing the privilege.
- Where a learner contravenes this policy by the unauthorised reproduction or distribution of material recorded on the college premises, they are deemed to be in breach of student conduct and will be subject to a student disciplinary hearing. Refer to Section 7.16 Student Disciplinary Committee of the College Quality Assurance Handbook.

- Unauthorised recording on college premises may also fall under the criminal offences' categories in some cases, e.g. copyright legislation.
- Undertake to destroy all forms of recording after programme completion.

2 & 3 - The Lecturer or College records an oral or visual presentation for teaching or assessment purposes.

- A lecturer authorised by the school will be allowed to record presentations on the following conditions:
- The class is made aware that the presentation is being recorded and may choose to ask (in advance) that their image or contribution is anonymised.
- The intellectual property remains with the college.
- The recording is for the College's own use and is not reproduced or distributed to any third party.

Procedure

Responsibility of Lecturers:

- To be aware of this policy & the possible consequences of refusing to grant permission i.e. that individual liability may apply and that their decision may be subject to scrutiny.
- Entitled to be informed by Registry if a certain learner has been approved to record under this policy.
- Will only be informed of the specific reason for the recording of presentations with the learner's explicit consent.
- Best practice would include the establishment of ground rules for professional behaviour in the classroom at the start of every year/module, which is discussed with students. This could include issues such as the recording of sessions, the purposes of this and how recordings can or cannot be used.
- Course information should include reference to arrangements for recordings.
- Inform all learners at the beginning of lectures when recording starts and ends. In addition, where the recordings will be posted. This will be Moodle, the online student portal. This should be done in such a way so as to avoid the identification of individual students with specific needs.

Learners

- All College led recordings will be in the online student portal, Moodle.
- In the case where a Reasonable Accommodation arrangement has been approved. As a matter of courtesy, the College advise the learner to inform the lecturer that you have been approved to record. If permission is denied, please inform the Registrar immediately. Where learners do not wish to disclose a Reasonable Accommodation directly to the lecturer the Registrar or their Programme administration Manager can do so on their behalf.
- The lecturer will inform all learners that the lecture is being recorded and learners may request that the recording is turned off when they are making a personal contribution.
- The learner will supply their own recording device and is responsible for its maintenance.
- The recording process should not interfere with the presentation.
- Any misuse of the privilege should be reported to the Registrar and Programme Administration Manager.

Intellectual property rights of the recordings shall remain with the college.

Procedure for visiting lecturers / guest speakers / dignitaries

All persons attending an IBAT College Dublin event that will be recorded and used for academic or promotion purposes should be informed of this policy on the recording of oral or visual presentations by the event organiser / lecturer.

In the case of a student using the recording under the policy of Reasonable Accommodations and if the speaker does not permit the recording of the event, it is the responsibility of the event organiser / lecturer, in conjunction with Registry, to ensure that the student in a Reasonable Accommodation arrangement is not disadvantaged.

Exceptions

In some cases, it may not be possible to record oral or visual presentations e.g. when confidential information is being discussed by staff and/or students.

In the case of recording under the policy for Reasonable Accommodations then The student should be informed by the lecturer when it is not possible to record oral or visual presentations and a clear justification should be provided. In situations where other students are permitted to take notes, the lecturer should ensure that the student under reasonable accommodation arrangements is not disadvantaged e.g. by implementing alternative methods or ensuring that notes are taken.

Retention & Deletion of recordings

Recordings of all presentations will remain on Moodle for the duration of the semester, at least until all resit opportunities have passed.

Recordings for assessment will be kept according to the document retention policy and then deleted.

Learners who have been approved for Reasonable Accommodation also undertake to destroy all forms of recording

Further information

If students or academic staff are unsure of the position in relation to the recording of oral or visual presentations, they are advised to contact the Registrar at DPO@ibat.ie

AP1.15 IBAT College Dublin Blended and Online Learning Policy

Document Title and Reference	IBAT College Dublin Blended and Online Learning Policy
Purpose	The source of reference for the policies, procedures, principles and practices upon which IBAT College Dublin quality assurance mechanisms are based.
Version	VP4.5
Author/Proposed/endorsed by	Registrar
Approved by	Academic Council
Approval date	March 23rd 2021
Endorsed by	Board of Governors April 13th 2021
Effective from	March 23rd 2021
Review date	August 2022

Introduction & Objectives

1.1 Introduction

The onset of CoVID19 necessitated a very quick response by HEIs to move students online to offset the disruptive nature in terms of programme delivery and meet our public health obligations.

Innovation in educational technology facilitated the timely execution of this unprecedented move. The move also expanded options for flexible learning experiences. For example, blended and online learning, afforded providers to offer a more flexible approach towards the delivery of learning. It also offered some advantages in terms of quality assurance, widening participation and programme enhancement. The way in which learning resources are used by learners can be more easily monitored and evaluated. Also, students that could not learn in face-to-face contexts now could participate.

In advance of seeking extension of scope to provide blended and online delivery of existing and new programmes this document specifies IBAT College Dublin's (IBAT) policy for the delivery of programmes leading to an award or to specified credits towards an award, delivered, supported, or assessed through means which may not require the student to attend on campus.

This policy is intended to support IBAT in developing flexible learning opportunities and providing access to higher education. It will also guide IBAT in managing the potential risks posed by challenges and complexities in the arrangements for blended and online learning programmes and to safeguard academic standards.

IBAT College Dublin is committed to providing equal opportunities for all staff and learners and is fully committed to the principles in The Equal Status Acts 2000-2018 ('the Acts') prohibiting discrimination in the provision of goods and services, accommodation and education. This policy demonstrates the College's commitment to equality of opportunity for all learners, across all its online and blended programmes.

1.2 Objectives of this Policy

The objectives of this policy are:

- To provide a framework for staff to engage with blended and online learning programme delivery;
- To ensure compliance with IBAT College Dublin's Quality Assurance framework in approval, delivery and monitoring of blended and online learning programme delivery;
- To ensure that the learning environment has the necessary operational supports for blended and online learning programme delivery;
- To ensure that the technical infrastructure is available for blended and online learning delivery;
- To ensure that staff are provided with the necessary training and support for blended and online learning programme delivery according to the relevant academic standard for programmes and awards;
- To provide guidance on instructional design for blended and online learning programme delivery;
- To ensure the legal responsibilities of the College have been met for blended and online learning programme delivery.

This policy needs to be read in conjunction with QQI Core Statutory QA Guidelines published in April 2016 and its supplemental topic specific guidelines, Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes.
In addition, Associated Policy 1.12 IBAT Policy on Recording of Oral or Visual Presentations complements this policy.

1.3 Definitions

IBAT have adopted the following definitions to apply throughout this policy for the key terms blended learning and online learning:

Blended Learning

The definition as contained in the QQI Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes (March 2018/QG8-V1) defines blended learning as.
"The integration of classroom face-to-face learning experiences with online learning experiences" (Garrison and Kanuak, 2004, p96). It further stated in these guidelines that as blended learning will always include a face-to-face element, it does not cover programmes where learning is fully online.

Online Learning

"A form of educational delivery in which learning takes place primarily via the Internet. Online learning can serve those who are geographically distant and without access to traditional classroom education, so it includes 'distance learning'. However, distance learners are not alone in benefiting from online learning, which is also commonly part of e-learning in mainly campus-based study programmes. In such cases, it may be referred to as blended learning" (Gaebel *et al.*, 2014, p17).

"Learning that is delivered or supported through the use of technology" (QQI, 2016, p27).

Fry (2001) extends the definition to include management of the programme, "Online learning is the use of internet and some other important technologies to develop materials for educational purposes, instructional delivery and management of program.

Hrastinski (2008) stated that the two types of online learning, namely asynchronous and synchronous online learning, are majorly compared but for online learning to be effective and efficient, instructors, organizations and institutions must have comprehensive understanding of the benefits and limitations.

Organisational Context

2.1. Scope

This policy covers all programmes of Higher Education that lead to a QQI award. It also incorporates Professional Diploma programmes offered in the College. An IBAT Professional Diploma is a focused, short duration practical course that consolidates, upskills and/or reskills learners in a professional area. They are stand-alone qualifications that do not lead to an award on the National Framework of Qualifications (NFQ).
The Policy covers teaching, learning and assessment of programmes with a blended or online mode of delivery. It is designed to safeguard academic standards and ensure support for staff and students engaged in blended and online learning programme provision. It is not our intention that this will be a permanent option for students and teachers, but rather an additional opportunity to complement, supplement and in some cases replace the existing delivery.

2.2 Legal and Policy Context

IBAT complies with the requirements of Ireland's national legislation, agreements, and regulations, including with Qualifications and Quality Assurance (Education and Training) Act 2012. The 2012 Act requires providers to have due regard to Quality and Qualifications Ireland (QQI) Quality Assurance guidelines in the development of their QA procedures and in the development of programmes of education and training. In June 2018 IBAT formally reengaged with QQI acknowledging IBAT's QA processes articulated in its Quality Assurance Handbook and a panel meeting with IBAT Senior management were satisfactory subject to a number of advised changes being considered.

Many studies have been conducted to document, debate and proffer what changes are required to be successful in the digital learning environment. This policy was informed by best practice through desk-based research and from the College being engaged in various fora e.g. National Forum for the Enhancement of Teaching and Learning, established by the HEA, with the aim of developing a cutting edge digital learning environment in all higher education institutions in Ireland. The IUA Digital Education Webinar Series and attendance at the National Academic Integrity Network all assisted us too in this regard.

2.3 Strategic context

The strategic goals as stated in IBAT College Dublin Strategic Plan to 2025 is:

- Engage with Influential employers in business and technology.
- Deliver a 5-year expansion plan.
- Leverage Global University Systems global footprint to grow the business.

In accordance with QQI (2018), Guideline 3. 1, the college's approved and published strategy should take account of the existing and planned development of blended and online learning provision. This policy is developed in the context of the College's published strategy and strategic choices in meeting the performance objectives above. The College's Strategy is outlined in chapter 1 of the College's Quality Assurance Handbook, V4.4 (available at: https://www.ibat.ie/quality-assurance.html)

Provision of blended and online delivery will meet employers' and employee's expectation for a more flexible response from HEIs to upskill and reskill the labour market. This is evident in the Springboard+ 2021 call for proposals.

> *Given the emphasis on upskilling people in employment in Springboard+ 2021, Providers should be cognisant of the fact that many participants will be unable to attend classes during regular business hours of 9-5pm, Monday to Friday. Therefore, it is expected that*

courses will be proposed based on flexible provision and/or at times of the week and weekend that suit the needs of learners in employment. (p8)

In terms of meeting the ambitious expansion plans. Offering our non-accredited professional diplomas online has facilitated a new market as people outside of Dublin are participating in these short duration programmes. Blended and online provision in accredited programmes would ensure programmes are more sustainable and make them accessible to those that can not commit to a full face-to-face delivery method.

IBAT is a college within its parent company, Global University Systems. Global University Systems (GUS) is an international network of 25 higher-education institutions, with over 75,000 students, brought together by a shared passion for accessible, industry-relevant qualifications. Collaboration is one of the 5 values of the College and it is our intention to collaborate with other GUS institutions. Blended and Online programme delivery is one way that possible collaboration can be achieved.

2.4 Principles

The development of blended and online learning provision is established within the context of the College's approved Strategic Plan to 2025, guided by the College values of:

- Learners' First: We have a deep commitment to our learners sits at the heart of everything we do. We seek and act on their feedback to enhance their experience.

And

- Empowerment: The College's educational philosophy is to inspire and empower the individual through the creation of independent and creative thinking, the development of knowledge, know-how, skill, competence for lifelong learning, in a nurturing learning environment

QQI guideline (2018), section 3.1 guided the development and implementation of procedures that ensure;

- all strategies and processes for the appointment, induction, training, professional development and appraisal arrangements for teaching and support staff are appropriate and specific to a blended or online learning environment.
- that teaching on a blended and/or online learning programme requires pedagogical and technological expertise. The College will ensure that academic staff are provided with the necessary staff development and support systems to function effectively in the delivery of blended and online learning programme provision.
- The College will create and maintain a technology enhanced learning and teaching plan for the delivery of blended and online learning, ensuring that the appropriate technical infrastructure and technical support for programmes with a blended and/or online learning delivery mode are in place.
- responsibility for compliance with legal and statutory obligations - to include but not limited – Protection of Enrolled Learners; Intellectual Property and Copyright legal obligations; Data Protection legislation including the General Data Protection Regulation (GDPR); applicable professional body requirements and local regulatory considerations in transnational provision.
- any arrangements for collaboration or partnership in the development, delivery, assessment or evaluation of blended and online learning provision are approved by the College and subject to appropriate and clear formal agreements as outlined in Chapter 9, Collaborative Arrangements and Other Parties Involved in Education and Training of the College's Quality Assurance Handbook.
- teaching, learning and assessment practices are accessible to students with disabilities. Apart from meeting our statutory obligations the College also wish to provide educational opportunity to a diverse range of students, recognising that exclusion can be caused by disability related to situational impairments and activity limitations.

Programme Context

3.1 Academic standards

IBAT College Dublin, through Academic Council, its Senior management team, in particular the College Principal, Registrar and Head of School ensure academic standards and quality assurance of programmes delivered through blended and online learning are delivered in accordance with its quality processes that underpin all of IBATs programmes, including validation, ongoing monitoring and periodic revalidation as outlined in its Quality Assurance Handbook (see https://www.ibat.ie/quality-assurance.html). The Quality Assurance Handbook also outlines the responsibilities to ensure the arrangements for the delivery of programmes and provision of support and assessment of students while ensuring that the academic standards of all awards are in accordance with QQI core statutory guidelines.

On an ongoing basis and in line with periodic review to its quality assurance processes and policies, IBAT will ensure;

- that procedures and regulations relating to Validation, Monitoring and Review are fit for purpose in a blended and online learning environment.
- that procedures and regulations are fit for purpose in a blended and online learning environment. For example, systems and processes are in place to verify the identity of students, manage remote assessments and across different time zones.
- that quality assurance systems to monitor and /or moderate standards are fit for purpose in a blended and online learning environment.
- that processes and regulations in respect of Access, Transfer and Progression are fit for purpose in a blended and online learning environment.
- that the college Learner Management System supports blended and online learning programmes and the quality assurance of a flexible learning experience.

3.2 Programme design and delivery

In accordance with QQI (2018) Guidelines 4: The College will ensure that:

- the teaching, learning and assessment strategies and delivery mechanisms adopted in blended and online learning delivery, should be specifically designed for this context.
- blended and online learning developments are learner centred and subject-led rather than technology led.
- teaching, learning, and assessment practices are accessible to all students.
- subject specific and educational scholarship informs the pedagogy and instructional design. Contact hours may no longer be an appropriate indicator related to teaching. The programme design will specify the required effort for the activities of teaching, content creation and moderation in blended and online learning delivery.
- all steps to ensure security and reliability of its online learning and support systems are in place.
- access to the college's online learning and support systems will be monitored and controlled by the College.

- Continuity of service delivery in terms of online learning and support systems are considered regularly through assessment of this risk at the College Audit & Risk Committee, a subcommittee of the Board of Governors.

Learner Experience Context

4.1 Student Information & Support

Learners are supported to make informed choices about participating in a blended learning programme and to develop the necessary independent study skills to successfully progress towards becoming an autonomous learner IBAT College Dublin will ensure:

- Prior to enrolment on a blended and/or online learning programme, prospective learners will be provided with information via the college website and contained in the Student Handbook it will be clear –
  - (i) the blend of learning that they will experience and the realistic commitment required of them to complete the programme as well as the pre-knowledge and technological skills necessary to participate;
  - (ii) the nature and extent of autonomous, collaborative and supported aspects of learning;
  - (iii) the hours when academic, technical or pastoral support is available;
  - (iv) the hardware and software required, e.g. detailing the required broadband specification;
  - (v) how much time learners are expected to commit to independent learning in order to successfully complete the programme;
  - (vi) the specific level of engagement expected for different elements of the blend, for example mandatory participation in online activities in order to demonstrate participation in collaborative learning activity, face-to-face attendance requirement, synchronous and asynchronous activities, autonomous learning etc.;
  - (vii) the extent to which face-to-face attendance is part of the blend is made clear to learners and/or other stakeholders such as funding, recognition or validating bodies.
  - (viii) the rules governing flexibility for learners, regulations in place to provide a unique student identity and protect student information.

  In addition, the College will ensure when a student is enrolled on a blended / online programme
- Face-to-face induction including an explanation of the concept of blended learning; where possible, staff who will deliver the online portion of the programme will be present at this induction. There will also be an opportunity for orientation to learning resources and other support to access them effectively and efficiently (including technical and academic support and guidance, as appropriate).
- Contacts (academic, administrative, technical) are identified and available to such learners at the times specified in their Student Handbook.
- Feedback will be sought regularly in both a formal and informal way to ensure learners are inducted correctly, they are capable of engaging and their learning and social experience is meeting the College's and more importantly the learners expectations.
- procedures and regulations as specified in the Student Code of Conduct are fit for purpose in a blended and/or online learning environment.
- Guidelines as specified in the College Policy on Recording of Oral or Visual Presentations are fit for purpose in a blended and online learning environment. It is essential that the College promotes dignity, courtesy and respect in their use and encourage gender sensitivity amongst both learners and teachers.
- All learners have an equitable, fair and realistic opportunity to achieve the intended learning outcomes –
  - (i) Where the online learning element is to be offered to learners based outside of Ireland, due diligence and risk management arrangements need to be robust and fit-for-purpose.
  - (ii) Reasonable accommodation and efforts are made to ensure blended learning experiences are accessible to all learners, including learners with disabilities.

Chapter 7, Supports for learners in the College's Quality Assurance Handbook and Associated Policy 1.9 College Data Protection and Record Management Policy provide further detail on supports available and how student data is treated.

4.2 Assessment of Students and Requirements

Assessments for blended and online learning programmes will be similar to those used for on-campus programmes with parity of standards being paramount. IBAT will ensure that the outcomes of assessment for a blended and/or online learning programme meets the specified academic level of the award as defined by the National Framework of Qualifications (NFQ).

Information on methods and criteria of assessment will be provided in the Student Handbook that accompanies their programme of study. In addition, the Student Handbook will inform students of the regulations and guidance on academic impropriety to avoid plagiarism. This stresses the importance that all learner's assessed work is their original work, particularly in cases where the assessment is conducted through remote methods.

The College will ensure security measures are in place to authenticate a student's work when designing assessment processes.

How online exams were conducted in December 2020 and January 2021

Students were required to sign an integrity pledge, adapted from UC San Diego Academic Integrity Office from a link recommended by QQI. This highlights the importance of academic integrity to students' and is based on trust. It puts the onus of academic integrity on the student and treats them as significant and valued stakeholders in the assessment process.

In addition, the College (the lecturer) retain the right to ask the student to develop an answer in more detail in the form of a Q&A session (integrity test). This would occur between the student & lecturer when the lecturer is correcting scripts.

The same Google tools that the student is familiar with from lectures are utilised for in-class tests and end of semester exams. An invigilator is present for the duration of the assessment. In recognition of the exams going online it was deemed appropriate to provide students with extra time, for example the 2 hour exams were 3 hours.

The Google tools were Google Classroom. Google Meets and Google Docs.

- ***Google Classroom*** –Each student was assigned to an exam as if they were classes with their corresponding resources.
  In the Resources Tab- Exam Regulations, the Exam Paper, Answer Book and an Excel work sheet, if applicable were available from here.
  Meeting link - shared with student, the lecturer and invigilator(s) of the exam. It was the student's responsibility to ensure they had access to Google Classroom. The College aided 1 student by offering a laptop to perform their exams when theirs broke.
  The College managed the start and finish time, releasing the paper, answer book and excel worksheet at 10.00 am and removing all students at 1.00 pm.

- ***Google Meets - Virtual Exam Hall***
  Access is via the App or via Google Classroom directly where the meeting link is displayed under the title. Here the Invigilator and Lecturer can see the student, take attendance, ensure the

registered student is the person taking the exam. They also ensure no other person and notes are present in the room where the student is taking the exam.

Log-in – Students are advised to access the Meets at least 15 mins (9.45 am on the morning of each exam). Invigilator can take attendance and read out the regulations to them.

Announcements - During the exam students are advised to check the chat room occasionally as it will be here that any announcements are made, e.g. a student asks for clarification on part b of a question. The invigilator liaises with the lecturer and all students are informed.

Sound – All students are requested to turn their mike off, so no disruption.

Vision – It is essential their webcam / camera is on for the duration of the exam. Any time it is not is noted in the Invigilator Report.

- ***Individual Google Documents*** – ***Student answers***

  Access - via Google Classroom each student answer book and excel sheet for calculations/rough-work/their thoughts etc.

  Students are informed –

(i) The answer book and sheet will be shared with the lecturer & invigilator(s). Shared Google Docs allow the invigilator/lecturer in real-time to review an individual script as the student is typing.

(ii) The Invigilator can message the student privately or type a comment directly on the student's script. Any such interactions will be noted in the Invigilator Report completed for each exam.

(iii) In addition, with SimCheck the individual answers submitted are dragged en-masse to be checked after the exam. Therefore, any potential academic integrity issues can be captured in real-time and if missed another opportunity after the exam through SIMCheck

Online proctoring software will be considered if blended and online provision will be permissible in the future.

Staff Professional Development in Online Teaching and Learning

5.1 Objective of professional development

To ensure that staff involved in teaching on a blended and/or online learning programme are appropriately qualified and supported the College will assess the level of competency at interview stage for new hires and through once-off assessment and engagement with existing staff to initially ascertain their competence and confidence in delivering blended &/or online content.

The European Framework for the Digital Competence of Educators (Redecker, 2017) https://ec.europa.eu/jrc/en/digcompedu will be the competency framework that will be employed to guide the College's appropriate level training of its staff to develop the academic and technological enhanced learning skills required to educate innovatively in a digital learning environment.

APPENDICES

Appendix 1: Glossary of Terms

Educational Technology

"The study and ethical practice related to the creation, use and management of appropriate technology for the design and delivery of education – including learning platforms, hardware, software and processes" (QQI, 2016, p27).

Flexible and Distributed Learning (FDL)

"A programme or module that offers a wholly at a distance, on-line, or blended learning experience, rather than requiring the learner only to attend classes or events at particular times and locations. Typically, it may not involve face-to-face contact between learners and tutors but instead uses technology such as the internet, intranets, broadcast media, CD-ROM and video, or traditional methods of correspondence - learning 'at a distance'" (QQI, 2016, p27).

Instructional Design

"The translation of pedagogical research into the design and testing of curriculum for FDL that is specifically centred on supporting the achievement of learning outcomes. Developing and implementing content (provided by academics) teaching and learning strategies and assessments for effective FDL delivery" (QQI, 2016, p28).

Learning Material

"The specific and/or specialist resources made available to learners through which the FDL course or programme is taught and learning opportunities are facilitated. Learning materials may be in any media such as hard copy, electronic, digital, audio or visual" (QQI, 2016, p28).

"The organisation that delivers FDL to learners and to whom fees are paid. In Ireland they may be an awarding body or another organisation that offers FDL on behalf of one or more awarding bodies" (QQI, 2016, p28).

Massive Open Online Courses

"An online course made freely available over the internet to potentially large numbers of learners at no charge. There are no entry criteria. MOOCs are not normally credit-bearing" (QQI, 2016, p27).

(Virtual Learning Environment)

"A site that hosts online resources and activities to support students' learning" (Ally, 2009, 291).

Appendix 2: National Teaching & Learning Forum Reports

The following is a comment synopsis of the findings in the reports from the National Teaching & Learning Forum that aided the drafting of this policy.

- **Building Digital Capacity in Irish Higher Education 2013-18 - National Developments and Key Perspectives (December 2018)**

This report:

(i) provided a record of recent developments in building digital capacity in Irish higher education.
(ii) shared perspectives of those who influence and shape teaching and learning in Irish higher education regarding digital developments in recent years
(iii) allowed work undertaken to date, and the perspectives of those involved, to inform future developments related to the digital dimension of teaching and learning in Irish higher education

https://www.teachingandlearning.ie/wp-content/uploads/Digital_Overview_2018_AW_180219.pdf

- **A Review of the Existing Higher Education Policy Landscape for Digital Teaching & Learning in Ireland (June 2018)**

The key findings in this report were;

(i) opportunities digital technology affords higher education.
(ii) Policy related challenges were identified in the areas of were: technology-enabled assessment, copyright and intellectual property rights, curriculum design, managing artefacts on a VLE, and student digital footprint and digital wellbeing.
(iii) Characteristics of enabling policies were outlined - implementable, situated in practice and reflective of institutional priorities. The review suggested that many existing policies do not recognise the practice context within which they are situated.
(iv) the challenges and opportunities related to digital teaching and learning were not often reflected in the language of existing policies.
(v) Enabling policies are permissive rather than restrictive and are intended to aid decision making, point to key challenges and help us to answer questions about how best to ensure consistent approaches and enhanced practice.
(vi) Reiterated that when institutions operate without a robust policy framework for digital teaching and learning, informal practices can emerge which are inefficient, confusing or risky. The development of clear policies is part of a wider strategy, outlined in A Roadmap for Enhancement in a Digital World.
(vii) Many institutions reported being in the process of developing policies for digital teaching and learning. It is therefore timely for a policy framework to enable enhanced digital teaching and learning in Irish higher education.
(viii) A step-by-step Guide to Developing Enabling Policies for Digital Teaching and Learning, recently published by the National Forum, aims to support those developing policies in a way that is mindful of both what is important to the HEI and also what is achievable in practice.

https://www.teachingandlearning.ie/wp-content/uploads/TL_EnablingPoliciesReview_WEB.pdf

- **Guide to Developing Enabling Policies for Digital Teaching and Learning in Higher Education (May 2018)**

This National Forum report is a comprehensive guide for any higher education institute in Ireland seeking to enhance or develop their digital learning polices and is available online https://www.teachingandlearning.ie/wp-content/uploads/2018/05/TL_Briefing_EnablingPolicyGuide_WEB.pdf. The report focuses on five themes including:

Theme one: Curriculum Design
The report includes models for curricular design for digital teaching and learning. Including the concept of Universal Design which responds to the diverse needs of student's on-campus as well as those at a distance. Links between curricular design and digital literacy skills required of staff and students for effective high-quality learning experiences and the growing role of students as co-creators as well as consumers of curricula are addressed. Presents resources and practice case studies illustrating the cost/benefits of particular forms of curricular design, and an explanatory framework of relevant digital pedagogies.

Theme two: IPR and Copyright Issues for Staff
The report will provide guidance for staff on the requirements of copyright in the development and use of digital learning resources, including Creative Commons copyright, the use of copyrighted material in a VLE context and Open Educational Resources. Individual Intellectual Property for the ownership of digital artefacts including digital resources, digital capture and storage of lectures.

Theme three: Digital Footprint and Digital Well-Being for Learners
This section will cover guidance on providing advice to learners on their digital presence and well-being, addressing digital engagement which is professional, ethical and safe for learners. This will draw a distinction between learners' social media activities and their academic activities. Considerations will include: digital socialisation and modelling of academic discourse in an online context; forms of online interaction and engagement; moderation of online discussion and approaches to "toxic postings". The work of the University of Edinburgh on Digital Footprint and Safety was identified as an exemplar resource.

Theme four: E-Assessment
This section will highlight the potential offered by mobile technology to facilitate engaged learning in large classes, provide feedback, enable more effective management of assessment including procedures for academic integrity as well as the analytics potential of e-assessment to illustrate cohort and individual engagement. This report will examine a typology of the different forms of e-assessment in terms of engagement, assessment management, analytics and academic integrity.

Theme five: VLE Management
The storage and archiving of curriculum information, student work and student contributions via discussion fora in institutional VLE's as well as distributed digital applications in post learning management systems settings are covered in the report. The report also focuses on developing policies for safe and reliable approaches for institutions in meeting their obligations for the reliability and security of systems for retaining student work

as well as responsibilities for ancillary digital resources or storage facilities used in teaching and learning, which sit outside the institutional VLE.

- **Teaching and Learning in Irish Education: A Roadmap for Enhancement in a Digital World 2015-2017 (March 2015)**

One of the key goals of the National Forum is to create a digital roadmap to help to guide institutions and organisations in the development of local and national digital strategies and to ensure alignment, coherence and a sense of common endeavour at a sectoral level. In 2017, the Forum launched the All Aboard Digital Skills in Higher Education roadmap and a suite of digital badges (see http://www.allaboardhe.ie/).
This report (link below) is designed to inform and guide senior managers, heads of department, schools or faculties and leaders within the higher education sector on developing a digital learning environment and building digital capacity to enhance teaching and learning across the sector. The roadmap identifies the key priorities for change and provides an informed framework for supporting organisations in addressing these priorities. The executive report can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2015/03/Digital-Roadmap-V2-EXEC-SUMMARY.pdf

- **Ireland's Higher Education Technical Infrastructure: A review of current context, with implications for teaching and learning enhancement (June 2017)**

This report provides a detailed snapshot of the current state-of-play of the technology infrastructure which supports teaching and learning in Irish higher education. The review seeks to enhance and inform the work of the National Forum in assisting Irish higher education institutions in their efforts to achieve a coherent digital future.
The full report can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2017/12/Final-Infrastructure-report-with-doi-web-ready.pdf

- **Using Learning Analytics to Support the Enhancement of Teaching and Learning in Higher Education (June 2017)**

The report looks at how learning analytics can be employed to the benefit of academic managers, staff and students. Employed intelligently, it can supply predictive models to better inform approaches to teaching, highlight what is working effectively and what is not and most importantly enable more focussed student interventions. The full report can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2018/01/Final_LA-Briefing-Paper_Web-with-doi.pdf

- **National Professional Development Framework for All Staff Who Teach in Higher Education (September 2016)**

This document describes the National Professional Development Framework for all staff who teach in Irish higher education. The framework provides guidance for the professional development (PD) of individuals and gives direction to other stakeholders (e.g. institutions, higher education networks, educational/academic developers, policy makers and student body representatives) for planning, developing and engaging in professional development activities. As we engage staff in developing their technology enhanced learning skills, there is an opportunity for staff to reflect and provide evidence of their learning journey mapped against the PDF five domains. The full report can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2016/09/PD-Framework-FINAL-1.pdf

- **Understanding and Supporting the role of Learning Technologists in Irish Higher Education (September 2016)**
  This briefing paper presents a summary of findings from a qualitative research project

conducted by the National Forum for the Enhancement of Teaching and Learning in Higher Education (National Forum) exploring the role (e of Learning Technologists (LTs) in supporting academic staff to enhance teaching and learning in Irish higher education. The College needs to identify staff for re-training in the LT skills area or recruiting Learning Technologists/Instructional Designers who can work with programme boards in developing their programmes for online learning. This paper is a guide on the role of a learning technologist and how they provide real value in developing the online learning experience. The full paper can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2016/09/LT-Briefing-Note-FINAL.pdf

- **Technology Enhanced Learning Survey (June 2015)**

This survey reports on what works and what doesn't work in technology enhanced learning and what inspires and encourages learning and creativity. This survey provides invaluable information about the current state of play in our institutions of higher education. The findings of the survey can be accessed online https://www.teachingandlearning.ie/wp-content/uploads/2014/03/TEL-FINAL.pdf

- **Learning Resources and Open Access in Higher Education Institutions in Ireland (July 2015)**

This report provides a considered account of some of the key issues which influence the sharing of open educational resources. These include questions of awareness and understanding of open educational resources at individual as well as institutional level, and the value placed on openness as a positive incentive for academic engagement. Acknowledging the complex interplay between these factors, the study suggests important practical steps to take forward OER engagement, including: awareness raising; professional development for academic staff; capturing excellent OERs and continuing relevant and targeted research to support particular OER initiatives. The full report can be accessed https://www.teachingandlearning.ie/wp-content/uploads/2015/07/Project-1-LearningResourcesandOpenAccess-1607.pdf

- **National Plan for Equity of Access to Higher Education 2015-197,**

The National Plan for Equity of Access to Higher Education 2015-197, provides a framework of actions that over the five years of the plan to improve equality of opportunity and to ensure that the student body in higher education reflects the diversity of Ireland's population. It sets new and increased targets for participation in higher education of those from the semi-skilled and unskilled socio-economic groups, of students with sensory disabilities, mature students and the wider adult population, as well as an increase in participation among Irish Travellers. In addition, it aims at an increase of part-time or flexible higher education participation and commits to a more consistent approach to access support across higher education institutions and progressing a number of projects in order to understand and to measure access data more effectively. A mid-term review of the plan is to be undertaken in early 2018.

- **The National Skills Strategy 2025**

The strategy aims to make Ireland internationally renowned for its talent, for its highly skilled and adaptive people, equipped with the higher order capabilities required in the 21st century workplace and for its openness to continuous learning. The full report can be accessed https://www.education.ie/en/Publications/Policy-Reports/pub_national_skills_strategy_2025.pdf

References

Ally, M. (2009) Mobile Learning Transforming the Delivery of Education and Training. Edited by M. Ally. Edmonton: AU Press. doi: 10.1111/j.1467-8535.2007.00809.x.

Fry, K. (2001). E-learning markets and providers: Some issues and prospects. Education+ Training , 43 (4/5), 233–239. https://doi.org/10.1108/EUM0000000005484. [Crossref], [Google Scholar]

Gaebel, M. et al. (2014) E-Learning in European Higher Education Institutions Results of a Mapping Survey Conducted in October-December 2013. Brussels.

Garrison, D. R. and Kanuak, H. (2004) 'Blended Learning: Uncovering Its Transformative Potential in Higher Education', Internet and Higher Education, 7(2), pp. 95–105.

Hrastinski, S. (2008). Asynchronous and synchronous e-learning. Educause Quarterly , 31 (4), 51–55. [Google Scholar]

IBAT College Dublin Strategic Plan to 2025 Available at: https://www.ibat.ie/quality-assurance.html

Springboard + 2021 Call for proposals. Available at: https://hea.ie/skills-engagement/springboard/

National Forum (2018a) Building Digital Capacity in Irish Higher Education 2013-18 - National Developments and Key Perspectives (December 2018) Available at: https://www.teachingandlearning.ie/wp-content/uploads/Digital_Overview_2018_AW_180219.pdf

National Forum (2018b) A Review of the Existing Higher Education Policy Landscape for Digital Teaching & Learning in Ireland (June 2018) Available at: https://www.teachingandlearning.ie/wp-content/uploads/TL_EnablingPoliciesReview_WEB.pdf

National Forum (2018) *Guide to Developing Enabling Policies for Digital Teaching and Learning in Higher Education*. Available at: https://www.teachingandlearning.ie/wp-content/uploads/2018/05/TL_Briefing_EnablingPolicyGuide_WEB.pdf.

National Forum (2015a) *Teaching and Learning in Irish Higher Education: a Roadmap for Enhancement in a Digital World 2015-2017*. Dubliln. Available at: www.teachingandlearning.ie.

National Forum (2015b) *Learning Resources and Open Access in Higher Education Institutions in Ireland*. Dublin. Available at: www.teachingandlearning.ie.

National Forum (2016a) *National Professional Development Framework for all Staff who Teach in Higher Education*. Dublin. Available at: www.teachingandlearning.ie.

National Forum (2016b) *Understanding and Supporting the Role of Learning Technologists in Irish Higher Education*. Dublin. Available at: www.teachingandlearning.ie.

National Forum (2017a) *Ireland's Higher Education Technical Infrastructure, A review of current content, with implications for teaching and learning enhancement*. Dublin. Available at: www.teachingandlearning.ie.

National Forum (2017b) *Using learning analytics to support the enhancement of teaching and learning in higher education*. Dublin. Available at: www.teachingandlearning.ie.

QQI (2016) *White Paper Statutory Quality Assurance Guidelines for Flexible and Distributed Learning*. Available at: https://qqi365-public.sharepoint.com/Publications/QA Guidelines for Flexible and Distributed Learning.pdf.

QQI (2018) *Blended Learning Programmes, Statutory Quality Assurance Guidelines for Providers of Blended Learning Programmes*. Dublin. Available at: http://www.qqi.ie/Publications/Publications/Statutory QA Guidelines for Blended Learning Programmes.pdf.

Redecker, C. (2017) *JRC Sciece for Policy Report European Framework for the Digital Competence of Educators (DigCompEdu)*. Edited by Y. Punie. Luxembourg: EU Science Hub. doi: 10.2760/159770 (online).

AP1.16 IBAT College Dublin Deferral Policy

Please note this policy needs to be considered in conjunction with the **College Terms & Conditions & Refund Policy**

What is a deferral?

- This is a period of time permitted by the College in agreement with an applicant or registered student whereby they are commencing their studies at a later date or taking a break during their studies.
- A deferral is only possible on the same programme and cannot be transferred to another programme.
- Deferrals are granted on a case-by-case basis.
- There is a limit on the number of deferrals which can be granted in any course. It cannot materially impact on next year's applicants or the operation of the current programme.

The financial implications

A deferral decision may be granted but the applicant or student must be familiar with their financial obligations. For example;

1. A deferral is not a valid reason to request a refund on fees paid. Fees will be retained and applied upon resumption of your studies.
2. If a student is on an agreed Payment Instalment Plan, payments will be made as per the agreed terms as stated in the Payment Instalment Plan regardless of the granting of a deferral.
3. For an applicant to secure their place on a programme and commence their studies at an agreed later date they will be required to make a deferral charge / deposit of €250 (Diplomas) / €1,000 (Higher Education).
   If you don't pay the deferral charge within the specified timeframe, the deferred entry place will be forfeited. You can, of course, apply again for the following intake / year in the normal way and be assessed in competition with other applicants.

How and to whom do I request a deferral?

Deferring is a big decision. Initially please forward your request by contacting to our Help Desk and open a ticket https://my.ibat.ie/helpdesk/public/create-ticket

Depending on your status – applicant / student you will be contacted by either a member of the student recruitment team or academic team. For example, in the case of:

1. If you receive an offer of a place but are not yet a registered student (Higher education programmes)
   a member of the student recruitment team will discuss your options.
2. If you are an existing student registered on a programme a member of the academic team with discuss your options.
   We would strongly urge you prior to making a deferral request to speak with a tutor or Head of School to discuss your options. You might benefit too from speaking to our Student Affairs Coordinator or Counsellor.
3. In the case of international / non- eu students you will be contacted by a member of the student recruitment team to discuss the fee and visa implications on seeking a deferral of your place.

Higher Education Programmes - Do I have to apply again the following year?

No. We will transfer your application to the following intake / year as agreed between you and Student Recruitment (if you deferred at offer stage) or with the School (if a student). Registry will inform the School and Student Recruitment if there are any implications in terms of Recognition of Prior Learning or if a student is admitted under transfer arrangements.

Professional Diploma programmes

As these are short duration programmes deferral requests are not permissible for any person who has attended more than 3 weeks of the 11-week duration.

AP1.17 IBAT College Dublin Social Media Protocol / Etiquette

Please also refer to AP 1.14 Policy on Recording of Oral or Visual Presentations, as IBAT is committed the privacy of all staff and learners and providing equal opportunities for all.

We welcome and acknowledge lecturers and students use of social media in teaching and learning. However, as a courtesy to all concerned and for others, we ask that you follow the IBAT College Dublin Social Media Etiquette.

Please do:

- The default assumption is that all presentations are "bloggable" and "tweetable". However, some lecturers or guest speakers may request that certain slides, or findings, be left out of the social media conversation. Please respect any such request.
- Please respect all participants, lecturer, and students – your posts are public and live forever.
- If you are tweeting or blogging during a session, please consider sitting near the back of the room to avoid distracting all others.
- Please mute your mobile phone/laptop/tablet volume to avoid disruptions.

Please do not:

- Post online any images, audio or video that have been recorded, without first having the presenter's explicit permission to post it.
- Photograph / screen grab lecturer slides and share them on social media without their permission.
- Capture, transmit or disseminate any research data presented as this can have a detrimental impact on future publication in academic journals.
- Tweet, or post elsewhere online, comments made by lecturers or students.
- Be rude or engage in personal attacks online.

Remember:

When posting on social media, remember that you must comply with relevant legislation such as the Copyright and Related Rights Acts 2000, 2004 and 2007, GDPR, and the Defamation Act 2009.

Thank you for following these social media guidelines.

AP1.18 IBAT College Dublin standards for materials and resources

Area: Planning Blended Learning delivery		
Aims: To ensure all stakeholders are engaged, aware and capable to meet and support the needs of the learner, as they must be at the centre of everything we do and central in the decision-making process		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Rationale for the programme / module - addresses a knowledge and skills gap that is causing, or will cause, a performance problem.	Inventory of existing resources and identification of additional resources required	ADDIE stage 1 (Analysis) & Quality Assurance Handbook 2021, V4.6 – Chapter 3 Programme Development, Approval & Validation
	Approved Budget for planned activities and resources required	
	Conducting primary & secondary research,	
Identifying the target learner and justifying why BL is most appropriate learning approach	Conducting primary & secondary research.	

Area: Developing Curricula and Materials		
Aims: To outline an instructional strategy (ADDIE methodology) that addresses the learning need identified in the planning stage. To design a curriculum that is participatory and activity-based to ensure that learners and lecturers are actively engaged in the learning process and learners develop the essential skills and knowledge needed		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Stakeholders are involved in the curriculum development process to ensure that strategies and systems are in place to support the learner before, during, and after delivery	Documentation of interviews, conversations, meetings, feedback, etc.	ADDIE Stage 2 & Quality Assurance Handbook 2021, V4.6 – Chapter 3 Programme Development, Approval & Validation

Area: Preparing for Implementation of Blended Learning		
Aims: To ensure successful operational and technical implementation of blended learning. To prepare learning activities to maximize the opportunity for learners to develop skills through real practice. To prepare learners, lecturers and staff for their roles before, during, and after the learning to ensure successful transfer of learning.		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Logistical arrangements & learning resources	Lecturer Common Room with links to resources, videos on training etc.	ADDIE Stage 3 & Quality Assurance Handbook 2021, V4.6 – Chapter 10 Staffing, Staff Development & Scholarship
	Learning Portal and Moodle populated with guides	
	Onboard training (lecturers) & Induction (learners)	
Trainer and facilitators are selected according to appropriate criteria and prepared.	Selection is documented and based on expertise required to implement the curriculum, including technical content and skills, training skills and experience.	

Area: Implementation of Blended Learning		
Aims: To ensure that blended learning happens as planned. To ensure that skills and knowledge are being transferred according to the curriculum. To ensure that lecturers and learners are actively engaged in the learning process. To ensure that feedback and supports are available throughout the learning.		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Technology required to implement learning intervention is available.	Planning in earlier stage identified any gaps / delay in technology implantation UAT Reports	ADDIE Stage 4 & Quality Assurance Handbook 2021, V4.6 – Chapter 4 Self-Evaluation, Monitoring & Review
Learning resources and logistical requirements	Documented the resources and requirements Student Handbook, Moodle and Learning Portal	
Learning is active and engaged	Written curriculum indicating participatory, activity-based methodology Lecturers are observed using the curriculum as written and actively engaging learners	
Knowledge & skills identified are assessed	As outlined in the programme assessment strategy, ensuring multiple methodologies are utilised	

All individuals involved in training (trainers and learners) receive feedback.	Observation & reports by CPD Coordinator so lecturer receives positive and corrective feedback, coaching, or mentoring Self-instructional training materials provided in the Lecturer Common Room. Distance learning may provide feedback electronically, from peers, site visits, etc. Learners provide feedback (electronically & paper-based) about lecturer, resources and support received from College.	

Area: Follow-up with learners		
Aims: : To ensure that learners have the tools and supports to engage on a blended learning programme.		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Learner support/ follow-up plan is included as part of the instructional strategy and describes the purpose of the follow-up, the methods to be used for follow-up, and the roles and responsibilities for carrying out learner follow-up.	Student Affairs Coordinator monitoring attendance (FTF component) & access logs (Online) and formally reaching out to ascertain why lack of engagement.	ADDIE Stage 5 & Quality Assurance Handbook 2021, V4.6 – Chapter 7 Supports for Learners

Area: Evaluation of the teaching and Blended Learning experience		
Aims: To assess learner performance. To assess the teaching and learner satisfaction on service delivery. To document successes, lessons learned, and recommendations to improve or apply best practices. To use evaluation information to make decisions regarding revisions to the curriculum and adjustments to the teaching and learning.		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
Documented process for evaluation included as part of the instructional strategy and	Documented processes for Programme Board Minutes	ADDIE Stage 5 &

describes what will be evaluated, how and where, when, who, and resources needed.	Annual Module Review & Development Plan (MRDP) Annual Programme Monitoring Report Programme Action Plan Template Minor Changes to Programme Approval Form	Quality Assurance Handbook 2021, V4.6 – Chapter 6 Teaching & Learning

Area: Documenting the teaching and learning of lecturers and learners		
Aims: To share knowledge and manage training and learning information. To report on results and successes to outside stakeholders. To maintain an inventory of information about training activities for future use.		
Standard	**As evidenced by**	**Reference on how to meet and document the standard**
A system is used to document and manage information about learners, lecturers, learning resources and other activities.	Updated Lecturer Common Room Presentations, recordings of ½ day workshops Central register for CPD and those embarking on teaching qualification	• Link to Moodle (Learners) • Link to Resource Centre • CPD Coordinator records on staff training

AP1.19 IBAT College Dublin IT Security User Policy 1.8

IBAT College Dublin
ICT Security Policy

Version 1.8 December 2024

Contents

Purpose

The purpose of this IT security policy is to protect the information assets of the IBAT College Dublin from all threats, internal, external, deliberate or accidental. The policy is aimed at:

- Safeguarding the availability, confidentiality and integrity of the College's information.
- Protecting the IT assets and services of the College against unauthorised access, intrusion, disruption or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing a governance structure with clear lines of responsibility and accountability.

The policy has been written to provide a mechanism to establish procedures to protect against security threats and minimise the impact of security incidents.

Policy Scope

The IT Security Policy covers procedures and standards relating to:

- IBAT College Information Assets
- IBAT College ICT Resources

The IT Security Policy applies to all stakeholders who use IBAT's IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices. The IT Security Policy also takes precedence over any policies which may be developed at a local level.

Roles and Responsibilities

IT Services are responsible for monitoring use of IBAT's ICT Resources in-line with this Security Policy.

IT Services and the Data Protection Officer (DPO) are responsible for enforcing effective operation of the Information Security Policy to ensure that information assets and technologies are adequately protected.

All stakeholders are required to demonstrate compliance to IBAT's Security Policy in order to protect the confidentiality, integrity, and availability of IBAT's Information Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to IBAT.

Confidentiality

Safeguarding the confidentiality of information through the protection of information from unauthorised disclosure with access only by entitlement.

Remote Working

With IBAT working from home is critically important to be aware of the risks around cyber-attacks from home, particularly ransomware. To combat this growing threat, we must all take the time to become educated on these threats and ensure we don't become victims.

What is Ransomware?

Ransomware is commonly spread via fraudulent emails, either as an infected email attachment containing malware or downloaded directly from the scammer's website. IBAT College has anti-virus scanning systems in place for detecting viruses on its network and Google is very good at filtering most of these emails, but with the current targeting of Irish HE Institutions we must all still be vigilant and exercise additional caution particularly with using company or personal computers at home for remote working.

It's also very important to realise that Ransomware is brutal and indiscriminate, it doesn't care if it infects an IBAT or personal computer, the result is the same, it will infect all documents, photos, videos and other important files so they are encrypted and cannot be opened or you're completely locked out of your computer; you are then held to ransom and asked to pay (usually bitcoin) to unlock your computer and/or unencrypted your files.

We have included these questions regarding ransomware and phishing which can help protect you against these types of cyber-attacks.

What is phishing?

Phishing is a form of online fraud. Scammers use phishing emails to trick you into giving away important information, such as your login details. They can then use these details to access your own data and login to IT systems, putting your own computer and potentially the College at risk

In a typical phishing incident, you may receive an email or pop-up message that claims to be from IBAT or another business or organisation that you may have previously dealt with for example eBay, PayPal, Revenue or Bank of Ireland. The message may ask you to 'update,' 'validate,' or 'confirm' your account information.

How can I identify a phishing email?

It is easy to be alarmed by a phishing email, they are designed to get us to act without question. They may appear to come from a legitimate business that you have previously dealt with or a colleague. Always trust your instincts, stay cautious, always take your time and consider the validity of the email, if an email offers something that looks too good to be true, it possibly is. Similarly, don't be tempted to respond hastily to an email which threatens to disable your account.

Phishing emails often have the following types of characteristics:

- They may use language like 'important notice', 'urgent update' or 'alert' or 'violation' with a deceptive subject line to persuade you that the email has come from a trusted source.

- They may contain messages that use threatening language, stating that your account will be disabled if you do not act.
- They may appear to come from someone in IBAT, but you should be aware that email addresses can be forged easily.
- They may copy content such as logos and images used on legitimate websites to make the email look genuine.
- They may contain hyperlinks that will redirect you to a fraudulent website instead of the genuine links that are displayed. If you see a link in a suspicious email message, don't click on it, if you are unsure, please contact IBAT IT Support at: it.support@ibat.ie
- All legitimate IBAT website addresses will always include ibat.ie as the main domain and will never include ".com", valid examples are shown below, these would typically be at the start of a legitimate IBAT web address:

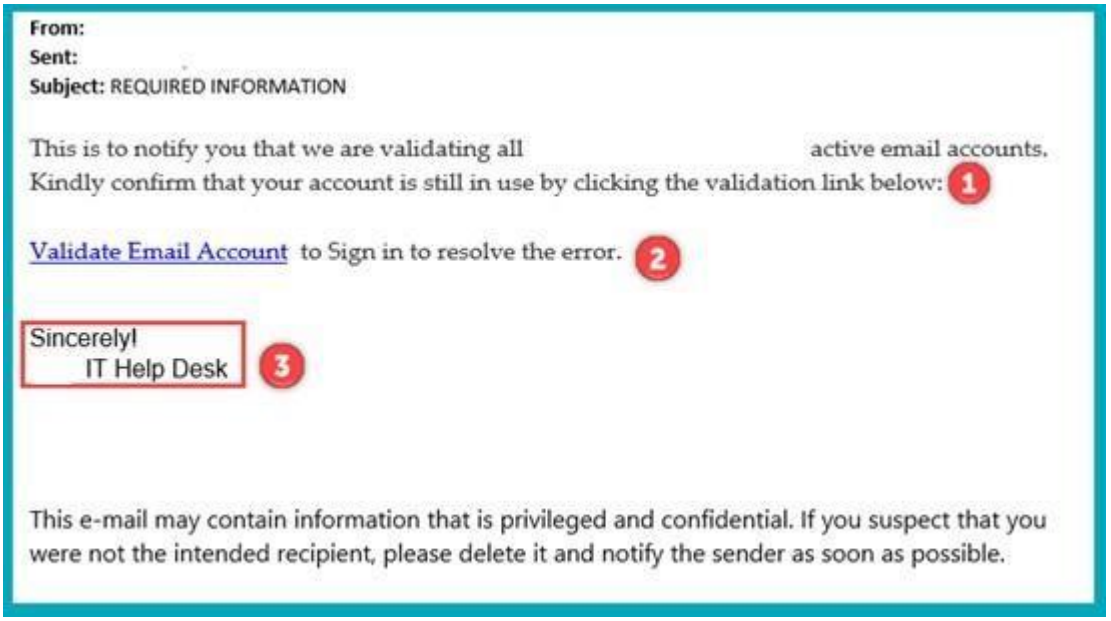
Look at the example of a phishing email message sent to students and staff below, this would be a typical example of the type of phishing email been sent to staff and students.

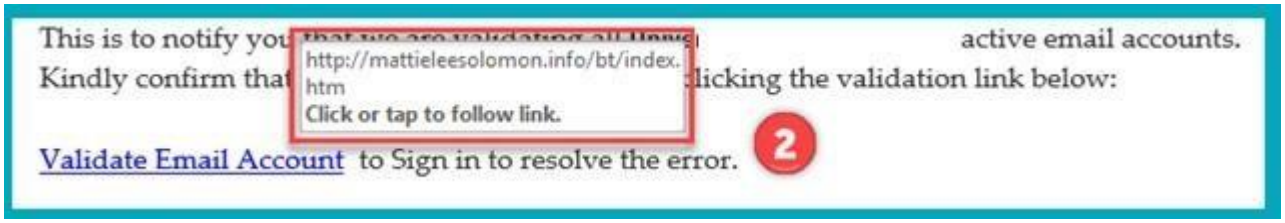
- **https://www.ibat.ie/**
- **https://www.ibat.ie/payments/**
- **http://intranet.ibat.ie/**
- **https://my.ibat.ie/helpdesk/**
- **https://my.ibat.ie/moodle/**
  - https://services.ibat.ie/ https://mail.google.com

And any legitimate web addresses from Google will always include "google.com"

- **https://classroom.google.com**
- **https://drive.google.com**
- **https://meet.google.com**
- **https://support.google.com/**

- If sent from IBAT, the sender email will always include a valid @ibat.ie address and will most likely be already known to you, or it will include a valid @ibat.ie email group such as: it.support@ibat.ie, studentsupport@ibat.ie, online.support@ibat.ie.
- IBAT will never ask you to verify any of your information over email or SMS, we can always do this face-to-face using Google Meet or MS Teams if necessary.
- If you are asked to go to an external link, you can check where this link will bring you by hovering over the link name.
  You can then see the address and confirm if the start of the URL matches the valid "ibat.ie" addresses shown above.
- Watch for unusual sign-off, we would never include "Sincerely!!" or "Help Desk"





Please spend 2 minutes viewing the YouTube Video below: https://youtu.be/YfiN_W8I1cE

What is ransomware?

Ransomware is a type of malware, where scammers aim to trick their targets into downloading malicious software on their computers in order to encrypt their files or lock them out of their devices. If you fall victim, the scammer demands you to pay a ransom in order to recover your files and/or regain access to your device.

Please spend 5 minutes viewing the YouTube Videos below:
https://youtu.be/Vkjekr6jacg https://youtu.be/kAfO4Rg2In4

What should I do if I receive a phishing email?

Please report any email that you believe is phishing to the IBAT IT Support (it.support@ibat.ie) as it may have also been sent to other IBAT staff members.
Remember treat any email that asks for your username and password with extreme caution.

What should I do if I have fallen for a phishing scam?

If you think you have fallen prey to a phishing email, immediately report the incident to the IBAT IT Support: it.support@ibat.ie

Change your password immediately, below is a link with the steps needed to change and/or reset your password. https://support.google.com/accounts/answer/41078?co=GENIE.Platform%3DDesktop&hl=en

I'm also including the link below again which outlines the importance of protecting your @ibat.ie Google account and the action needed to add 2 step authentication, if this still needs to be done, then please follow the instructions provided. https://www.google.com/landing/2step/

Backup your Data

Backup your data, files and devices regularly – this will help you recover any lost or damaged data/files should you fall victim to ransomware.

It's important to note that the responsibility for backing up data held on personal devices needs to done by staff member as we cannot backup personal devices or those outside the IBAT network. Please ensure all company files are stored in the designated company drives and folders (Z: Datafile and S: Shared) on the IBAT Network.

Please note that all IBAT staff have their own personal network drive/folder (H: Drive), any files that cannot be stored into the shared company drives/folders above should be store in the personal drive/folders provided so they are included with the daily backups.

All staff also have an @ibat.ie Google account which includes Google Drive, many staff have been using Google Drive extensively for sharing files, it can also be used as a secondary backup, so in the event that your computer is compromised and files become infected you still have these files safely stored in the cloud with Google Drive and separate from your computer.

Be Vigilant

Do not download or open files from unsolicited emails. If you receive an email with attachments you were not expecting from someone you know, check with that sender before acting on the email.

If it's been sent your @ibat.ie email then please report it to IBAT IT Support (it.support@ibat.ie) as it may have also been sent to other IBAT staff members.

Some more top tips to protect your privacy.

- **Keep work and social life separate.** Only use your IBAT email address and accounts for work related purposes. Use a personal email address for social and domesitic websites and apps.
- **Use unique, long and complex passwords or passphrases**. IBAT passwords must be unique. The length and complexity of your passwords can provide an extra level of protection for your personal information.
- **Take care what you share.** Periodically check the privacy settings for your social networking apps to ensure that they are set to share only what you want, with whom you intend. Be very careful about putting personal information online. What goes on the Internet usually stays on the Internet.
- **Go stealth when browsing**. Your browser can store quite a bit of information about your online activities, including cookies, cached pages, and history. To ensure the privacy of personal information online, limit access by going "incognito" and using the browser's private mode.
- **Using Wi-Fi?** If only public Wi-Fi is available, restrict your activity to simple searches (no banking!) or use a VPN (virtual private network). The latter provides an encrypted tunnel between you and the sites you visit.
- **Should you trust that app?** Only use apps from reputable sources. Check out reviews from users or other trusted sources before downloading anything that is unfamiliar.
- **Know your rights.** Become aware of your data protection rights and the responsibilities of those who hold and process your personal details. You can find more information here.

Personal Information is like money, Value it, Protect IT

Think before you act: Be wary of communication that implore you to act immediately, offers something that sounds too good to be true or ask for personal information.

Guard your date of birth and telephone number: These are key pieces of information used for verification, and you should not share them publicly. If an online service or site asks you to share this critical information, consider whether it is important enough to warrant it.

Get two steps ahead: Switch on two-step verification or multi-factor authentication wherever offered to prevent unauthorised access.

Secure your devices: Use strong passwords or passcodes or touch ID features to lock your devices. Securing your device can help protect your information if your device is lost or stolen and keep prying eyes out.

Think before you app: Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value? just like money. Be thoughtful about who gets that information and how it's collected through apps.

Get savvy about WiFi hotspots: Public wireless networks and hotspots are not secure – this means the possibility exists that anyone can see what you are doing on your laptop or smartphone while you are connected to it. Think about what you are doing and if you would want another person to see it. If you use public WiFi , think about using a virtual private network (VPN) that provides a more secure WiFi connection.

Now you see me, now you don't: Some stores and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi and Bluetooth when not in use.

Share with Care

What you post can last a lifetime: Before posting online, think about how it might be perceived now and in the future and who might see it. Share the best of yourself online.

Own your online presence: Set the privacy and security settings on web services and devices to your comfort levels of information sharing. It's ok to limit how and with whom you share information.
Click here for more information.

Be aware of what's being shared: Be aware that when you share a post, picture or video online, you may also be revealing information about others. Be thoughtful when and how you share information about others.

Post only about others as you have them post about you. The golden rule applies online as well.

Email Policy

The purpose of this Policy is to set out the conditions under which the College's email system – Google Mail – may be used, and the principles for managing messages created or received as part of the College's business. It applies to all staff and other authorised account holders.

Electronic Mail is a tool provided by IBAT College Dublin and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of College email accounts evidences the user's agreement to be bound by this policy.

Ownership

All @ibat.ie email addresses, associated accounts, work-related emails and instant messages are the property of the College. Ownership allows the College the right to access/monitor emails and, if necessary, their content.

Personal data

Google Mail and its related applications (e.g. Google Drive, Google Calendar, Google Meet) are hosted in the cloud. Google handles all personal data in line with its Privacy Policy (www.google.co.uk/policies/privacy/) and adheres to the European Union Privacy Shield (www.privacyshield.gov/EU-US-framework). The College is signed up to the JANET contract with Google, which addresses the requirements of Irish Data Protection legislation.

Legislation

Please see the Appendix for a brief description of the main pieces of legislation that have a bearing on the use and transmission of emails.

Conditions of use

Email facilities are provided to support learning, teaching, research, administration and approved business activities of the College. Refer to page 8 regarding personal use conditions.

Account Creation

Name used to create e-mail account:

IBAT College email accounts are created based on the official name of the staff or faculty member as reflected in Student Management System and HR records. Requests for name changes to correct a discrepancy between an email account name and official College records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by- case basis by the IT Support Team: itsupport@ibat.ie.

Responsibility:

- Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.
- Staff are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding College matters sent from an administrative office, faculty, or staff member is considered to be an official notice.

Set-up considerations:

Emails and instant messages (which are saved in Google Apps, if one or more of the people involved in the conversation have the history set to "on the record") are potentially disclosable to external parties and statements must not be made that could expose the College to legal liability or damage its reputation.

Legal Framework:

Emails are subject to the same laws and policies that apply to other forms of communication, including the relevant data protection legislation and the Freedom of Information Act 2014, and must be composed using the same degree of care as would be used for a formal letter.

All communication undertaken on behalf of the College is subject to the College's Data Protection and Privacy policy (available at https://www.ibat.ie/privacy-policy.html). In addition account holders must comply with the G Suite Acceptable Use Policy (available at www.google.com/apps/intl/en/terms/use_policy.html).

Security

Users are responsible for the security of their mailboxes.

Vigilance (Viruses):

Although emails are automatically scanned for virus content and spam, account holders are expected to take reasonable measures to prevent the introduction and transmission of computer viruses. These include:

- not opening attachments received from unsolicited or untrusted sources;
- not transmitting attachments known to be infected with a virus;

Strong Password:

Users should use strong passwords and must never disclose their passwords to others. A strong password contains at least one upper case letter, number and symbol. If it is necessary to provide another user with access, delegation should be employed, which enables authorised access without the sharing of passwords.

Two-factor authentication:

In addition to a strong password, the College strongly advises the use of two-factor authentication for Google accounts (https://www.google.com/landing/2step/).

Managing SPAM:

Google Mail automatically helps identify spam and suspicious emails and will place these into your Spam folder (label). Staff can also teach Google Mail what is spam by highlighting emails in your inbox and

clicking the "Report Spam" button. This will send the message to your Spam folder and remove it from your inbox, and Google Mail will continue to do the same if you receive future emails from that sender. If you make a mistake and do not want the message to be in Spam, click the "Not Spam" button to move it back into your inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message.

Lock your workstation:

All staff should lock their workstations (Ctrl+Alt+Del on Windows) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

Report:

Users may not monitor, intercept or browse the messages of others, unless authorised to do so. The IT Support Team should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to his/her account.

Prohibited use

Staff should always use their College email address to conduct College business, as Google Apps Mail is webbased and can be accessed from any location with internet access. This is to ensure that the College has a record of all business correspondence and to enable the College to back up work-related emails for business continuity purposes. In addition, provision has been made for offline access to emails, when necessary.

The College email facilities **must not be used** for:

- using or attempting to use the accounts of others without their permission;
- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing, libellous or defamatory;
- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- the creation or transmission of material that brings the College into disrepute;
- the creation or transmission of material that is illegal;
- the incitement of violence;
- unauthorised transmission to a third party of confidential material concerning the activities of the College;
- the transmission of unsolicited commercial or advertising material, chain letters or other junk mail;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- excessive or unreasonable personal use.

Other examples of improper use of the email system include:

- generating or facilitating unsolicited bulk email;
- infringing on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- violation, or encouraging the violation of, the legal rights of others or national laws;

- any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- interfering with the use of the email services, or the equipment used to provide the email services, by students or other authorised users;
- altering, disabling, interfering with or circumventing any aspect of the email services;
- tests or reverse-engineer the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- content that:
    (i) constitutes, fosters, or promotes pornography ;
    (ii) is excessively violent, incites violence, threatens violence, or contains harassing content;
- creates a risk to a person's safety or health, creates a risk to public safety or health;
- compromises security, or interferes with an investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- misrepresents the identity of the sender of an email;
- using or attempting to use the accounts of others without their permission;
- collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);
- use of the service to distribute software that covertly gathers or transmits information about an individual;
- conducting business for profit under the guise of the College;
- Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of IBAT College Dublin.

This list is not exhaustive. Inappropriate use such as activities referred to above may result in the suspension of a user's email facilities for as long as necessary to conduct an investigation. The instigation of formal action under the staff disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

Personal use

Permission & Restrictions:

Modern technology makes it easy to check personal email accounts on mobile devices, anywhere, anytime. Staffs are permitted a limited level of personal use within their work email account, but should be mindful that it must not:

- be detrimental to the main purpose for which the facilities are provided;
- conflict with College objectives, values, or interests;
- conflict with the College's rules, regulations, policies and procedures;
- conflict with an employee's obligations to the College as their employer;
- involve personal financial gain or be of a commercial or profit-making nature that could take the individual away from their own work);

- involve significant use to pursue personal legal or domestic issues.

How to manage personal mails:

- Staff should ensure that either any messages addressed to or sent from their work email account for private purposes are clearly identified as personal and filed within a separate folder, or are deleted as soon as practicable. Separating personal emails from work-related information (or deleting them) will help delegated access users to avoid breaching the privacy of others when checking mail on behalf of absent members of staff.
- Staff who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.
- Staff should be aware that personal email sent from a work account may still need to be disclosed if the College receives a request under relevant information disclosure legislation (e.g. Freedom of Information and Data Protection legislation etc). Likewise, information disclosure requirements may also apply to work related emails sent from a personal email account. For this reason, personal email accounts should not be used for sending or receiving work related emails.

Distribution group emails

Group distribution list are a useful means of conveying information and, when necessary, important and urgent messages to all staff of the College. It is, however, important that the facility is used appropriately and only by designated and authorised staff.

These all-staff emails are for the timely dissemination of information considered important to all staff and may encompass the following categories:

- Important IBAT College related news or announcements
- GUS newsletter and corporate correspondence
- Academic correspondence and information relevant to each school
- Information relevant to the operation or suspension of IT systems
- Health and safety matters
- Access issues where buildings may be affected
- Governance and legal compliance matters
- Critical incidents

Use of distribution lists or 'reply all' features of email should only be used by authorised staff and only for legitimate purposes as per these guidelines.

Monitoring

Account activities (e.g. storage usage, number of log-ins) are monitored by Google and all messages are routinely scanned (for viruses, spam and other security threats) to assist with the effective operation of the email system. This process is completely automated, and no human intervention is involved. The use of all personal information by Google is governed by its Privacy Policy (www.google.co.uk/policies/privacy/).

The College, as the domain administrator for Google's facilities, may have access to information held in an email account. The College reserves the right to access this information in the following circumstances:

- in connection with a criminal investigation;
- in connection with a properly authorised and evidenced investigation in relation to breaches or alleged breaches of the College's rules on use (including but not limited to whistleblowing, fraud and bribery);
- to meet legal or statutory requirements;
- in a situation (such as prolonged staff absence) where access is required to enable the College's business to continue; (Refer to page 3, point 7 about Delegate Access).
- in an emergency situation.

Where there is evidence of an offence, it will be investigated in accordance with the College's disciplinary procedures.

Confidentiality

Appropriateness & Attachments

Email, like any other form of communication, is not completely secure and its confidentiality cannot be guaranteed: messages can be intercepted by third parties, wrongly addressed, forwarded accidentally and forwarded by recipients to third parties. Before transmitting information of a confidential nature, users should assess whether it is appropriate to transmit the data in the email itself, or whether it should be in a document attached to/linked from the email. If documents containing sensitive information are sent from the College's network to external addresses, then staff must password protected and encrypt the attachments first.

For guidance on how to encrypt documents please review these websites links:
https://www.groovypost.com/howto/geek-stuff/password-protect-encrypt-microsoft-office-2010documents/

https://www.groovypost.com/howto/password-protect-encrypt-office-2016-documents-excel-wordpowerpoint-o365/

Forwarding:

Before forwarding messages, whether externally or internally, staff should consider whether the authors of the messages would expect or be willing for this to happen. Staff should also consider whether the transmission of the information would breach the privacy of an individual or infringe copyright. In cases where it is necessary to send a message to a number of individuals – some (or all) of whom do not work for the College – care must be taken to prevent the recipients' email addresses from being disclosed **Transparency:**

The **'BCC' facility** should be used to ensure that the addresses of the recipients cannot be viewed by each member of a distribution list.

Monitoring and record keeping:

Work-related emails are records of the College's actions and decisions, and must be managed as efficiently, and in the same way, as paper and other electronic records. There should be consistent, coherent controls in place to meet business and accountability needs, as well as to ensure legal compliance.

Messages must be checked regularly, prioritised and answered as promptly as possible. They should also be stored logically to ensure that information can be managed effectively and readily retrieved in response to enquiries (such as Data Protection and Freedom of Information requests).

Staff is encouraged to tag emails with Labels, Stars and importance tags to aid the management of current mail and retrieval of archived mail.

Access by Google:

Google also retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy

http://www.google.com/a/help/intl/en/admins/use_policy.html

Training and Guidance

Online training on the use of Google Mail and other G Suite applications are available at:

https://gsuite.google.com/training/

Email Signatures

In order to present a consistent and professional image to those with whom the College corresponds, staff is expected to adhere to corporate guidelines when creating their email signature.

The logo used in the signature will be reviewed regularly and, where appropriate, updated to reflect those that most enhance our reputation. Staff will be informed when the logos to be used in the approved email signature change.

The format is as follows;

- Sign off
- Name | Role
- IBAT Logo
- Campus Address
- Contact details – Campus Main Switch, Direct Dial (if applicable), e-mail, website.

For example

Kind regards

John Doe | **Lecturer**

16-19 Wellington Quay, Temple Bar, Dublin 2, Ireland

T +353 1 807 5055 **DD** +353 1 246 1508 **E** **john.doe@ibat.ie** **W** www.ibat.ie

Retention & Deletion

For further information please refer to Associated Policies 1.9, College Data Protection and Record Management Policy and 1.10 Data Retention Schedule that accompany the College Quality Assurance Handbook, 2021 V4.5

It is the responsibility of all staff to ensure that messages with continuing value are saved. Emails cannot be treated as a single series with a single retention period: the length of their retention must be determined by their subject matter or business purpose, as is the case with any other electronic or paper record.

Retention decisions should take into account business/operational needs, legal and regulatory requirements, accountability and transparency expectations. Messages relating to complaints, appeals, disputes and grievances should be retained as long as there is a need to preserve an audit trail.

The risk implications of deleting messages must be considered, as well as the obligation to comply with Data Protection legislation.

Google offers unlimited email storage, but this must not be abused. Staff is obliged to review their emails (both their inbox and their archived mail) on a regular basis to ensure that those that have served their purpose are deleted. Messages that are no longer needed should be moved to the Bin. Staff should be aware that all items placed in the Bin will be automatically deleted after thirty days and cannot be recovered. Whilst information is held in the Bin, it will be considered still accessible and may therefore have to be disclosed (in the period before erasure) in response to requests made under Freedom of Information or Data Protection legislation.

Shared email accounts

In departments where several staff are responsible for work activity and require access to the same emails, sharing access to a single account can make it easier to answer messages promptly and manage them effectively when individual members of the team are away.

Using a shared email delegated account should also simplify the process of sorting accounts when staff leaves: if team members keep the majority of their emails in a shared mailbox, less time should be required for reviewing individual accounts when staff leave the College.

Each shared delegated email account requires a primary contact that is responsible for the overall management of the mailbox, ensuring there are effective procedures in place for controlling incoming and outgoing messages.

Staff or departments can request temporary delegated shared access to email accounts. Staff requesting these types of account will be required to submit user information, rationale for account and expiration date to their Line Manager or Head of School (HoS)for approval. Following approval, a request can be logged with the IT Support Team: itsupport@ibat.ie

Staff should be aware that when they allow a colleague delegated shared access within Google Mail, they are granting full read and write access to that person. However, any emails sent from an email address using delegated permissions will need to be clearly identified as to the real author for each recipient.

Unless otherwise agreed between the user and their delegated colleague, access should only be used in times of absence or emergency. Anyone who is granted access to another user's account must respect the confidentiality of that account and must not view data that is clearly of a personal nature.

Absence from the College

In cases of planned absence, staff must set up an out-of-office message giving alternative contact details to ensure that enquiries can be answered promptly.

Illness or other unforeseen circumstances

In cases of illness or other unforeseen circumstances, where it is not possible to make any preparations for being away from the office, delegate access to your account will be through your line manager or the IT manager and not accessed by your peers.

The following actions are required by line management or HoS in the case of academic staff:

- Set up an automatic reply. To do this, the line manager or HoS should log a request with the IT Support Team, requesting that an auto-reply is added to the relevant staff account and supplying the exact text for the reply.
- Set up an auto-forwarding facility, if necessary. To request auto-forwarding, the line manager or HoS should similarly log a request with the IT Support Team: itsupport@ibat.ie
- Ensure emails received in the intervening period are dealt with, as necessary. If the line manager or HoS needs to gain access to the account to check whether there are business emails requiring attention, they should log a request with the IT Support Team: itsupport@ibat.ie

Leaving a department or the College

When members of staff leave the College, it is their responsibility to delete all personal messages and, in some instances, transfer access to appropriate colleagues.

Staff should be aware that, once they have left the College, they will no longer have access to their @ibat.ie email account, as this is the property of the College. It is therefore important that they remove all their personal emails – any items of a personal nature that they wish to retain should be forwarded to a private email address in advance of their departure.

It is also the responsibility of each staff member to ensure that an appropriate out-of-office response is set up to inform senders that they have left the organisation and give them alternative options for submitting their enquiry to another email address or department.

Expiration of Accounts

Staff and students may leave the College for a variety of reasons, which has implications on the duration of email privileges or when an account expires. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, the College reserves the right to revoke email privileges at any time.

- Staff members who leave the College will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.
- Staff who have retired from the College will have email privileges removed effective on their last worked day.
- Students who leave the College without completion of their studies may keep their email privileges for one academic year from the last term when they were registered.
- Expelled students - If a student is expelled from the College, email privileges will be terminated immediately upon the directive of the Registrar's Office.

- Students who have graduated from the College will be permitted to retain their email account for a period of one year, follow which their account will be terminated.

Local File Backup Policy

Background

Local Data Files are files that are IBAT College related information and mission critical data that are saved on your **Local Hard drive**.

What is a Local Hard Drive? A physical hard disk that is in your own PC where you save all the information on a specific folder such as "My Documents"

What is H Drive or Home Folder? This is a folder located on the network and not in your local hard drive. Home folder or Personal folder is part of the Z Drive Data File \ Users folder where you can save Corporate Data from your local hard drive to your own Home Folder.

Home folder is only accessible to the folder owner and cannot in any way be accessed by other staff.

A disaster can happen anytime such as Physical Error, Virus Infection, Natural or Environmental that will cause all your files to become accessible or possibly be deleted and become unrecoverable and unusable. Each staff has been provided with a Personal Folder on the network without limitation to be able to copy, backup or synchronize their data to and from.

Losing your data is disastrous, so regular backup is a must so that if disaster occurs, the IT Department are able to restore your data based on your latest backup.

Objective

- To ensure business continuity for all staff when disaster occurs.
- To provide information for all staff of the importance of regular back up.
- To be able to Backup and Restore Local Data Files when disaster strikes on staff Local PC or Laptop.
- To provide awareness for staff in terms of Data Protection and Security.

Policy

All Local Data Files that are ONLY related to company should be saved or backup to H Drive or HOME FOLDER on the File Server.

It is generally recommended that you store your most Corporate Data in your H Drive or Home Folder in the network.

Staff and Lecturers are given a personal storage on the network which should be used for storing and backing up company related files.

A simple copy and paste procedure is the only process for now to copy or back up your files from the "My Documents" folder to your H Drive or Home Folder.

Simple Copy and Paste Procedure

1. Make sure the file is **Closed**.
2. **Right click** the file on your local drive.
3. Choose **Copy** (nothing will happen after this.)
4. **Go** to your **H Drive or Home Folder** and choose a folder where to copy the file.
5. **Right click** the correct folder destination and choose **Paste.** Please see policy no. D11 for Overwriting Files.
6. You can also copy a whole folder but be careful on the overwriting process.

User Responsibility

It is the responsibility of all staff to keep his or her Local Files to be backed up regularly in the H Drive or Home Folder.

- It is the responsibility of all staff to back up ONLY company related data and not personal data.
- It is the responsibility of all staff to protect and secure their Local Data File stored on their Local Hard Drive
- IT Department DO NOT recommends backing up Corporate Data in an external storage or USB stick without permission from the IT Department for security reasons.

IT Department and Exceptions

- Special software will audit file access and back up time for each staff in order to monitor the time and date of your last backup so that we can restore whatever latest information based on the audit and in your last backup.
- IT Department is responsible for backing up all Corporate Data saved on the Z Drive including staff Home Folder.
- IT Department is responsible for keeping the Corporate Data secure and should be backed up regularly in accordance to the Network Backup Policy.
- IT Department will NOT be held liable for any loss, deleted, corrupted data on your local drive if this policy has not been followed accordingly.
- IT Department is NOT responsible for accidental OVERWRITING with your existing files on the H Drive or Home Folder. Please ensure that before deciding whether you will overwrite the file/s & folder/s or not, please review the changes first and the target document itself.
- Windows Systems detects if the file you are copying already exists on the destination. A confirmation will pop up on the screen that will compare the file that you are copying and the file already there, and this gives you the decision if you want to overwrite it or not.
- Windows will give you detailed comparison of the file size, date and time of modification etc. So you must be aware of these details. Overwritten files are irreversible.

- IT Department treats every single document as highly classified information and should not be opened and read, sent out by email or distributed without proper authorization from senior management.
- IBAT College Dublin reserves the right to review and or require change of any identification and/or authentication process for compliance with this policy.

Privacy Policy and (GDPR) Review and Approval

IBAT College Dublin takes the protection of your personal data very seriously and are committed to protecting and respecting your privacy.

The EU General Data Protection regulation (GDPR) and the Data Protection Act 2018, gives people the right to know what information is held about them, and requires IBAT to ensure that personal information relating to living individuals is handled properly, held in confidence and is protected from inappropriate disclosure to third parties.

As part of our legal obligations we have published Staff, Student and General Privacy notices. Where required local privacy notices will be issued to inform individuals about what personal data is gathered, how it is used, stored and retained.

Data Controller

IBAT College Dublin ("IBAT "also referred to in this notice as "we" or "us") and is part of The Global University Systems B.V. group of companies which is made up of different legal entities, details of which can be found at: www.globaluniversitysystems.com .

IBAT registered address is: IBAT College Dublin, Wellington Quay Campus, 16-19 Wellington Quay, Dublin 2, Ireland.

Our Data Protection Officer

If you have any questions about IBAT's privacy policies, please contact the Data Protection Officer at IBAT College Dublin, Wellington Quay Campus, 16-19 Wellington Quay, Dublin 2,

Ireland. E-mail DPO@ibat.ie

How to Use This Privacy Policy

IBAT holds and processes information about many different types of people such as its current, past or prospective employees, visitors to is website, applicants, students and alumni & supporters. It also processes personal information for a variety of reasons. IBAT may also be required by law to collect and use certain types of personal information to comply with statutory requirements. For each category of personal data process you will find the following headings:

- What types of personal data we collect?
- How we use your information?
- What we use your information for?
- Where we collect your information from?
- Who we share your information with?
- How long do we keep your personal information?
- How can you access, amend or take back the personal data that you have given to us?
- How do we store and transfer your data internationally?

- What are cookies and how do we use them
- How to reject cookies

More information on how IBAT collects and uses personal information can be found in the relevant privacy notices below:

Types of personal information we collect

We collect, use and store different types of personal information about you, which we have grouped together as follows:

Types of personal information	Description
Publicity Available Data	Details about you that are publicly available, such as on Companies House or elsewhere on the internet
Marketing Data	Details about your preferences in receiving marketing communications from us
Consents Data	Any permissions, consents or preferences that you give us
Usage Data	Information about how you use our website, products and services

How we use your information

Cookies

This website uses Cookies; for more information on our cookies use, please read our cookies statement on our website: https://www.ibat.ie/cookie-policy.html

Generally

The table below outlines how we use your personal information and our reasons. Where these reasons include legitimate interests, we explain what these legitimate interests are.

What we use your information for	Our reasons	Our legitimate interests
To provide you with information you may ask for	Consent Legitimate interests	To fulfil enquires you might make of us
To allow you to register for updates or for notifications of blog posts on our website	Consent Legitimate interests	To provide you with information that you may request from us
To allow you to register for events that we may be hosting	Consent Legitimate interests	To hold events, such as seminars, webinars, open days or corporate hospitality to promote our business and its services

To allow you to register as a member of our alumni network	Consent Legitimate interests	To operate and develop our alumni network and the activities of our alumni programme

To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	Legitimate interests	To provide efficient client care and services To ensure that our technology operates efficiently and without error To assess which of our services may be of interest to you and to tell you about them To develop new products and services and improve existing ones
To manage our relationship with you which will include notifying you about changes to our privacy notice and our website terms and conditions	Legitimate interests Contract performance	To provide efficient client care and services To keep you updated about changes in the legal terms that apply to the use of our website For record keeping and firm management
To manage the systems that contain our marketing database To manage marketing preferences and keep our records up to date	Legitimate interests	For data management for marketing and business development purposes To improve our systems and services To seek feedback To seek your consent when we need it to contact you
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	Legitimate interests Consent	To improve our marketing strategy and the services that we provide
Sharing information with third parties - to facilitate data-gathering to improve our educational services, our website, and our marketing efforts.	Legitimate interests	For the purposes of IBAT's legitimate business interests such as managing and developing its business

Where we collect your personal information from

We may collect personal information about you from the following sources:

- Directly from you
- Cookies – see our cookie statement which can be accessed from our website

- Analytics providers, such as Google Analytics

Who we share your information with

We may share your personal information with the following third parties:

- Our agents and service providers who we use to help us with marketing.
- Event organisers (if we are organising an external event which you are attending)
- The police and other law enforcement agencies
- Relevant regulators, including the Data Protection Commission (DPC) in the event of a personal data breach
- Other companies owned or jointly owned by Global University Systems

How long we keep your personal information

Where we use your personal information for marketing purposes we will retain your personal information for so long as we have your consent to do so (where we use your personal information with your consent in order to send you marketing messages) or, in other cases, for so long as we have a legitimate business or commercial reason to do so (unless you ask us to stop).

Where you withdraw your consent to receiving marketing materials or otherwise ask us to stop marketing we will add your details to a suppression list which ensures that we remember not to contact you again.

To withdraw your consent e-mail studentsupport@ibat.ie

If you withdraw your consent to receiving marketing materials or ask us to stop our marketing activities, we will still communicate with you for other purposes in the normal course of any other relationship we may have with you.

International transfers

As a global company, we hold some personal information concerning our suppliers and their affairs within Ireland. We do work with agents and service providers who may process your personal information on our behalf outside the EEA. If your information is processed outside the EEA, we will ensure that it is protected to the same standards as if it were being processed within the EEA by putting in place a contract with our agents and service providers that provides adequate safeguards.

If you require more information or have any queries, please contact our Data Protection Officer at: DPO@ibat.ie

How long we keep your personal information

Your personal data is held securely on InterActive Pro's alumni and supporter database, which is accessible by a limited number of staff and is secured.
We ensure we have appropriate data sharing agreements in place before sharing your personal data. We do not sell your personal data to third parties under any circumstances, or permit third parties to sell on the data we have shared with them. InterActive Pro is committed to working in a transparent, ethical, responsible and honest way.

Applicants and Students Privacy Notice

IBAT College Dublin (IBAT) takes the protection of your personal data very seriously and are committed to protecting and respecting your privacy.

When processing your Personal Data, IBAT is obliged to fulfil individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation (the GDPR), the Data Protection Act 2018 (DPA), and other relevant legislation and regulations (collectively "Data Protection Law").

Purpose of this Notice

This privacy policy sets out the basis on which any personal data we collect from you, or that you or any third parties provide, will be processed by us. We may withdraw or modify this notice at any time and we may supplement or amend this notice by additional policies and guidelines from time to time. We will notify you if this notice is amended.

IBAT also referred to in this notice as "we" or "us") is a data controller (which means we are responsible for deciding how we hold and use your personal information) of your data and is part of The Global University Systems B.V. group of companies which is made up of different legal entities, details of which can be found at https://www.globaluniversitysystems.com .

"**Personal data"** refers to information relating to a living, identifiable individual. It can also include **"special categories of data",** which is information about your racial or ethnic origin, religious or other beliefs, and physical or mental health, the processing of which is subject to strict requirements. Similarly, information about criminal convictions and offences is also subject to strict requirements.

"**Processing"** means any operation which we carry out on your personal data e.g. obtaining, storing, transferring and deleting.

2. Your personal information

We hold a range of personal data about you, some of which you provide to us direct and some of which we receive from third parties, such as CAO, where relevant. **See below for further details of personal data we receive from third parties.** Examples of categories of personal data which we hold are: your contact details, prior educational experience/attainment, immigration information (e.g. passport details, language proficiency), where relevant, health information (including any disabilities) and other equality-monitoring data you provide to us. In addition, if you come to study with us, we process data about your academic performance, attendance and progression, and where relevant, breaches of our policies (e.g. academic or other misconduct concerning IBAT -related activities).We also process contact and educational details after you have completed your programme or your activities with us are otherwise terminated.

The purposes for which we process your personal data and the legal basis

When you are an applicant, we process your personal data for the purposes of assessing your eligibility to be offered a place on one of our academic or professional programmes.

If you take up a place at IBAT, we process your personal data for the purposes of providing our academic or professional programmes and related services.

If you are unsuccessful or do not take up a place at IBAT, we will retain your personal data in line with our retention schedules for statistical and audit purposes or in the event of a complaint or an appeal.

We only process data for specified purposes and if it is justified in accordance with data protection law. The table below lists the various purposes for which we process personal data and the corresponding

justification for it. Some processing of your personal data is justified on the basis of contractual necessity. In general, this applies to personal data you provide to us to process your application and if enrolled, to monitor academic performance.

Without that information, we would be unable to provide you with your chosen academic programme and related support services. Some personal data is also required to fulfil our legal obligations regarding immigration. A failure to provide that information would prejudice your application for a student visa.

No	Purpose	Legal basis/ justification
1	Assessing eligibility to undertake our academic or professional programmes.	Processing is necessary for the purposes of taking steps prior to entering into a contract with us
2	Supporting applicants through the application process and providing further information on the services we can offer	Necessary for negotiating to enter into a contract and legitimate interests in providing support to applicants
3	Provision of academic programmes and related services (including IT and library services).	Necessary for performing a contract, i.e. to provide your chosen academic programme. This can be a contract with us or a contract between you and your home institution ("contractual necessity")
4	Identifying students and assisting them in trying to succeed in their learning via the dashboard system.	Contractual necessity and legitimate interest in assisting our students to succeed in their studies
5	Assessment of academic progress and performance (including attendance), and where necessary providing support	Contractual necessity
6	Financial Administration (including provision of loans and bursaries)	Contractual necessity
7	Administration of extenuating circumstances procedures.	Contractual necessity
8	Administration of complaints, academic appeals, interruption and withdrawal, fitness to study and fitness to practice procedures.	Contractual necessity
9	Immigration matters.	Necessary for us to comply with our legal obligations in relation to students who hold student visas. Such processing may also be in the public interest.

10	Making reasonable adjustments for disabilities and providing relevant support to students with ill health and providing wellbeing support.	Explicit consent.

No	Purpose	Legal basis/ justification
	This includes processing special category information.	
11	Employability Support	Contractual necessity and our legitimate interest in assisting our students and alumni to progress in their careers.
12	Regulating IBAT's community (including dealing with misconduct under our procedures for academic and other misconduct including disciplinary procedures)	Contractual necessity and our legitimate interest in maintaining academic standards and the good order of IBAT community.
13	Obtaining payment of fees.	Contractual necessity and our legitimate interest in obtaining payment for the services we provide.
14	Protecting our property and assets (e.g. by dealing with misconduct)	Necessary for our legitimate interest in safeguarding our property and assets.
15	Providing appropriate I.T. and other infrastructure facilities e.g. a virtual learning environment	Contractual necessity: legitimate interest in providing a proper infrastructure to support the provision of academic or professional programmes and related student services.
16	Communicating with students	Contractual necessity and our legitimate interest in marketing IBAT and promoting student welfare.
17	Registering alumni to maintain an alumni network	Necessary for our legitimate interests in maintaining an alumni network, and marketing
18	To facilitate data-gathering to improve our educational services, our website, and our marketing efforts. Recorded lectures and webinars maybe used for training and marketing purposes at the college's discretion to improve customer service and experience.	IBAT's legitimate business interests such as managing and developing its business

There may be other processing in addition to the above, for example, when you access our website which uses cookies or when we take photos of our events and publish them. This is done on the basis of our policies and we will inform you about such processing at the time when the data is obtained or as soon as reasonably possible thereafter.

Where the basis of processing your personal data is contractual necessity and you fail to provide the personal data in question, IBAT may not be able to process your application or provide you with the programme for which you have applied. A failure to provide immigration-related data may result in failure to obtain a student visa for those students who require it.

Personal data received from third parties

No	Data	Source
1	Contact details and attainment.	CAO, call agents
2	Your immigration status.	The Irish Naturalisation and Immigration Service (INIS)
3	Transcripts - details of programmes undertaken or being undertaken at another institution; attainment.	Another institution and/or secondary/high schools.
4	Medical, mental health, accessibility-related and similar information. This is special category personal data. We only obtain this information from third parties if you give us consent to do so or if it's a matter of life and death.	Another institution, medical practitioners and/or family members
5	Your financial status.	Student Loans Company.
6	Details of any IBAT -associated complaint	Office of the Independent Adjudicator, and/or Competition & Consumer Protection Commission.
7	Information required to assess eligibility for courses i.e. from employers or sponsors.	Employers or sponsors.
8	Details as to how you are performing in your apprenticeship job.	Your employer if you are an apprentice
9	Details as to how you are performing on placement.	Your placement provider
10	Details of performance at a partner institution including attendance and disciplinary issues.	International study abroad or exchange programme partner or collaboration partner.

Recipients of personal data

On occasion we may need to share your data with third parties. The following table lists what information we may share with whom

No	Recipients	Data which we may share with them
1	Companies within the group	Contact details, Course information where students and graduates are interested in entrepreneurship activities and relevant employability activities
2	Placement providers	Your CV as well as any accessibility and assistance requirements and related information.
3	Co-curricular and/or extracurricular excursion providers	Accessibility and assistance requirements and related information.

4	Your employer if you are an apprentice.	Details as to how you are performing in the academic part of your apprenticeship.

No	Recipients	Data which we may share with them
5	Your employer or sponsor if you are a sponsored student.	Details as to how you are performing and attendance in your course.
6	External examiners.	Identification details and exam papers.
7	Turnitin.	Identification details and assessment papers in order to detect plagiarism
8	Education and Skills Funding Agency if you are an apprentice.	Student details including course and employer information and academic progression.
9	End point assessor if you are an apprentice	Identification details and assessment details.
10	The Irish Naturalisation and Immigration Service (INIS)	Passport details; contact details; programme details including attendance, placement details and work experience; fees and housing details
11	Data processors i.e. third parties who process personal data on our behalf e.g. software providers or marketing service providers	Application details; attendance records or contact details which are not retained by the third party
12	Local Authority (including the electorate office).	Contact details and course details where there's a legal basis.
13	Student Loans Company.	Contact details and course details including progression.
14	IBAT's insurers and internal and external auditors, Health and Safety Executive in respect of accidents or incidents connected with the company.	Student details and details in relation to any incident.
15	Regulatory bodies, where you are on a professional programme	Contact details, attendance and progression information and potentially disciplinary or fitness to study or fitness to practice issues
16	Government agencies i.e. The Revenue Commissioners*	Contact details and potentially other information if requested where there is a legal basis.
17	Police*.	Contact details and potentially other information if requested where there is a legal basis.
18	Potential employers or other companies requesting a reference or confirmation of qualifications	Attendance, progression and performance details including disciplinary or academic misconduct issues or breaches of the IBAT's regulations.

No	Recipients	Data which we may share with them
	(Your explicit consent will be requested)	
19	Close family, next of kin and emergency services where there is an emergency situation such as illness or serious injury	Personal data including potentially special category data if necessary
20	UK and international educational institutions which IBAT partners or collaborates with to deliver placements, study abroad programmes, dual awards, franchised or validated awards or any articulation or progression agreement.	Contact details, attendance, progression and performance details and details of any disciplinary or academic misconduct issues or breaches of IBAT's regulations
21	Higher Education Authority (HEA) and Government Departments such as the Department of Education and Skills for analysis of student data or to carry out statutory functions	Personal details, progression and performance details, details of the Destination of Leavers' Survey. The privacy notice for the Department of Education and Skills can be found here https://www.education.ie/en/Privacy_Information_and_Disclaimer/ The privacy notice for HEA can be found here https://hea.ie/about-us/data_protection/
22	External debt collection agencies, in relation to student debts where IBAT's own recovery attempts have proven unsuccessful	Contact details and details of debt

** This will only be shared on request and where there is a legal basis for doing so.*

Overseas transfers of personal data (i.e. outside the European Economic Area (EEA)

Where possible, we aim to hold personal data relating to students within the EEA. Where any of your personal data is transferred outside the EEA it will be subject to a legally binding data sharing agreement and to an adequacy decision by the European Commission (country, territory or specified sectors), or other appropriate safeguards as set out in Article 46 of the GDPR.

Retention of data - The length of time that we keep your personal data for is set out in the College Data Retention Schedule, please contact DPO@ibat.ie for more information.

Your rights as a data subject - As a data subject, you have the following rights in relation to your personal data processed by us:

- To gain access to your personal data;
- To rectify inaccuracies or where appropriate, given the purposes for which your data is processed, the right to have incomplete data completed;
- To have your personal data erased. This is a limited right which applies, among other circumstances, when the data is no longer required, consent has been withdrawn and/or the processing has no legal justification. There are also exceptions to this right, such as when the processing is required by law or in the public interest;
- To object to the processing of your personal data for marketing purposes. You may also object when the processing is based on the public interest or other legitimate interests, unless we have compelling legitimate grounds to continue with the processing.
- To restrict the processing of your personal data. This is a limited right which will apply in specific circumstances and for a limited period.
- To obtain a copy of your data in a commonly used electronic form if the data is processed by automated means and the processing is based on your consent or contractual necessity.
- To not have decisions with legal or similar effects made solely using automated processing, unless certain exceptions apply.

Where we are relying on your consent to process your data, you may withdraw your consent at any time. Your requests will be considered at the latest within one month.

Exercising your rights, queries and complaints

For more information on your rights, if you wish to exercise any of the above rights or for any queries you may have or if you wish to make a complaint, please contact;

Written: FutureLearn DPO, 30 Holborn, London EC1N 2LX.

E-mail: dpo@futurelearn.com

Complaints to the Data Protection Commission

The Data Protection Commission is the national independent authority which oversees compliance with tData Protection Legislation. You have a right to complain to the Data Protection Commission (DPC), about the way in which we process your personal data. You can make a complaint on their website https://www.dataprotection.ie/

Appendix - Legislation

1. Copyright

Email messages and attachments are subject to the laws regarding copyright, including the Copyright and Related Rights Act, 2000. Staff must ensure that they do not circulate or store material that infringes the intellectual property rights of a third party.

2. Data protection

The General Data Protection Regulation (GDPR) 2018 covers personal data that can identify a living individual and relates to not only facts but also opinions expressed about individuals. Under this legislation, individuals have the right to ask to see the personal data held about them. Care should therefore be taken in writing emails that may contain personal data as the emails, whether held in an individual's email account or on the College server, will have to be released if requested. More details about data protection can found at:

- https://www.ibat.ie/privacy-policy.html
- Refer to Associated Policies 1.9, College Data Protection and Record Management Policy and 1.10 Data Retention Schedule that accompany the College Quality Assurance Handbook, 2019 V4.4
- GDPR, IBAT COLLEGE DUBLIN & YOU – Guide to Staff on GDPR and their rights

3. Defamation

Email is a form of publication and therefore the laws of defamation and libel apply. Material to be transmitted via the email system must be free from such statements: it should not contain anything that could be seen as insulting or damaging to the personal or professional reputation to an individual or a group of people.

4. Discrimination

Users must ensure that they do not include comments that could be considered discriminatory under the terms of the Employment Equality Acts 1998 - 2015.

6. Hacking

Hacking activities are offences under the Criminal Justice (Offences relating to Information Systems) Act 2017 which gives effect to the conditions outlined in the EU Cybercrime Directive and the Council of Europe Convention on Cybercrime. Under the terms of this legislation, it is an offence to gain unauthorised access to any program or data held in a computer, and to impair the operation of programs or the reliability of data.

7. Harassment

Messages must be free from any content that could be considered harassing, threatening, abusive or insulting. Content of this type is an offence under the Criminal Justice and Public Order Act 1994 and the Protection from Harassment Act 1997.

8. Obscenity

It is a criminal offence to publish any material that is pornographic, excessively violent or that comes under the provisions of the Post Office (Amendment) Act 1951 which also falls under the Communications Regulation Act 2007.

Email Policy

The purpose of this Policy is to set out the conditions under which the College's email system – Google Mail – may be used, and the principles for managing messages created or received as part of the College's business. It applies to all staff and other authorised account holders

Electronic Mail is a tool provided by IBAT College Dublin and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of College email accounts evidences the user's agreement to be bound by this policy.

Ownership

All @ibat.ie email addresses, associated accounts, work-related emails and instant messages are the property of the College. Ownership allows the College the right to access/monitor emails and, if necessary, their content.

Personal data

Google Mail and its related applications (e.g. Google Drive, Google Calendar, Google Hangout) are hosted in the cloud. Google handles all personal data in line with its Privacy Policy (www.google.co.uk/policies/privacy/) and adheres to the European Union Privacy Shield (www.privacyshield.gov/EU-US-framework). The College is signed up to the JANET contract with Google, which addresses the requirements of Irish Data Protection legislation.

Legislation

Please see the Appendix for a brief description of the main pieces of legislation that have a bearing on the use and transmission of emails.

Conditions of use

Email facilities are provided to support learning, teaching, research, administration and approved business activities of the College. Refer to page 8 regarding personal use conditions.

Account Creation

Name used to create e-mail account:

IBAT College email accounts are created based on the official name of the staff or faculty member as reflected in Student Management System and HR records. Requests for name changes to correct a discrepancy between an email account name and official College records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis by the IT Support Team: itsupport@ibat.ie.

Responsibility:

- Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.
- Staff are expected to read email on a regular basis and manage their accounts appropriately. An email message regarding College matters sent from an administrative office, faculty, or staff member is considered to be an official notice.

Set-up considerations:

Emails and instant messages (which are saved in Google Apps, if one or more of the people involved in the conversation have the history set to "on the record") are potentially disclosable to external parties and statements must not be made that could expose the College to legal liability or damage its reputation.

Legal Framework:

Emails are subject to the same laws and policies that apply to other forms of communication, including the relevant data protection legislation and the Freedom of Information Act 2014, and must be composed using the same degree of care as would be used for a formal letter.

All communication undertaken on behalf of the College is subject to the College's Data Protection and Privacy policy (available at https://www.ibat.ie/privacy-policy.html). In addition account holders must comply with the G Suite Acceptable Use Policy (available at

www.google.com/apps/intl/en/terms/use_policy.html).

Security

Users are responsible for the security of their mailboxes.

Vigilance (Viruses):

Although emails are automatically scanned for virus content and spam, account holders are expected to take reasonable measures to prevent the introduction and transmission of computer viruses. These include:

- not opening attachments received from unsolicited or untrusted sources;
- not transmitting attachments known to be infected with a virus;

Strong password:

Users should use strong passwords and must never disclose their passwords to others. A strong password contains at least one upper case letter, number and symbol. If it is necessary to provide another user with access, delegation should be employed, which enables authorised access without the sharing of passwords.

Two-factor authentication:

In addition to a strong password, the College strongly advises the use of two-factor authentication for Google accounts (https://www.google.com/landing/2step/).

Managing SPAM:

Google Mail automatically helps identify spam and suspicious emails and will place these into your Spam folder (label). Staff can also teach Google Mail what is spam by highlighting emails in your inbox and clicking the "Report Spam" button. This will send the message to your Spam folder and remove it from your inbox, and Google Mail will continue to do the same if you receive future emails from that sender. If you make a mistake and do not want the message to be in Spam, click the "Not Spam" button to move it back into your inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, co- worker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message.

Lock your workstation:

All staff should lock their workstations (Ctrl+Alt+Del on Windows) when away from their desk, even for short periods. Computers which cannot be locked must not be left unattended whilst logged-on.

Report:

Users may not monitor, intercept or browse the messages of others, unless authorised to do so. The IT Support Team should be informed immediately, if a suspected virus is received or a user becomes aware that someone has gained unauthorised access to his/her account.

Prohibited use

Staff should always use their College email address to conduct College business, as Google Apps Mail is web- based and can be accessed from any location with internet access. This is to ensure that the College has a record of all business correspondence and to enable the College to back up work-related emails for business continuity purposes. In addition, provision has been made for offline access to emails, when necessary.

The College email facilities **must not be used** for:

- using or attempting to use the accounts of others without their permission;
- the creation, transmission or storage of text, images and other material that is offensive, obscene, indecent, discriminatory, harassing, libellous or defamatory;
- the transmission of material that infringes the intellectual property rights of another person, including copyright;
- the creation or transmission of material that brings the College into disrepute;
- the creation or transmission of material that is illegal;
- the incitement of violence;
- unauthorised transmission to a third party of confidential material concerning the activities of the

College;

- the transmission of unsolicited commercial or advertising material, chain letters or other junk mail;
- activities that corrupt or destroy other users' data or disrupt the work of others;
- activities that violate the privacy of others or unfairly criticise or misrepresent others;
- excessive or unreasonable personal use.

Other examples of improper use of the email system include:

- generating or facilitating unsolicited bulk email;
- infringing on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- violation, or encouraging the violation of, the legal rights of others or national laws;
- any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- intentionally distributing viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- interfering with the use of the email services, or the equipment used to provide the email services, by students or other authorised users;
- altering, disabling, interfering with or circumventing any aspect of the email services;
- tests or reverse-engineer the email services in order to find limitations, vulnerabilities or evade filtering capabilities;
- content that:
  - (i) constitutes, fosters, or promotes pornography ;
  - (ii) is excessively violent, incites violence, threatens violence, or contains harassing content;
- creates a risk to a person's safety or health, creates a risk to public safety or health;
- compromises security, or interferes with an investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- misrepresents the identity of the sender of an email;
- using or attempting to use the accounts of others without their permission;
- collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);
- use of the service to distribute software that covertly gathers or transmits information about an individual;
- conducting business for profit under the guise of the College;
- Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of IBAT College Dublin.

This list is not exhaustive. Inappropriate use such as activities referred to above may result in the suspension of a user's email facilities for as long as necessary to conduct an investigation. The instigation of formal action under the staff disciplinary procedures may follow and, in certain circumstances, legal action may be taken.

Personal use

Permission & Restrictions:

Modern technology makes it easy to check personal email accounts on mobile devices, anywhere, anytime. Staffs are permitted a limited level of personal use within their work email account, but should be mindful that it must not:

- be detrimental to the main purpose for which the facilities are provided;
- conflict with College objectives, values, or interests;
- conflict with the College's rules, regulations, policies and procedures;
- conflict with an employee's obligations to the College as their employer;
- involve personal financial gain or be of a commercial or profit-making nature that could take the individual away from their own work);
- involve significant use to pursue personal legal or domestic issues.

How to manage personal mails:

- Staff should ensure that either any messages addressed to or sent from their work email account for private purposes are clearly identified as personal and filed within a separate folder, or are deleted as soon as practicable. Separating personal emails from work-related information (or deleting them) will help delegated access users to avoid breaching the privacy of others when checking mail on behalf of absent members of staff.
- Staff who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.
- Staff should be aware that personal email sent from a work account may still need to be disclosed if the College receives a request under relevant information disclosure legislation (e.g. Freedom of Information and Data Protection legislation etc). Likewise, information disclosure requirements may also apply to work related emails sent from a personal email account. For this reason, personal email accounts should not be used for sending or receiving work related emails.

Distribution group emails

Group distribution list are a useful means of conveying information and, when necessary, important and urgent messages to all staff of the College. It is, however, important that the facility is used appropriately and only by designated and authorised staff.

These all-staff emails are for the timely dissemination of information considered important to all staff and may encompass the following categories:

- Important IBAT College related news or announcements
- GUS newsletter and corporate correspondence
- Academic correspondence and information relevant to each school
- Information relevant to the operation or suspension of IT systems
- Health and safety matters
- Access issues where buildings may be affected
- Governance and legal compliance matters
- Critical incidents

Use of distribution lists or 'reply all' features of email should only be used by authorised staff and only for legitimate purposes as per these guidelines.

Authorised Research

Research is fundamental aspect of College life. Students, staff and the College can conduct research or be subjects in a research project. Any staff member contacted on their College email address for the purpose of voluntary recruitment into studies must ensure the research has received a favourable

opinion from a research ethics committee. This is the only form of authorised research permitted using @ibat.ie email accounts.

Monitoring

Account activities (e.g. storage usage, number of log-ins) are monitored by Google and all messages are routinely scanned (for viruses, spam and other security threats) to assist with the effective operation of the email system. This process is completely automated, and no human intervention is involved. The use of all personal information by Google is governed by its Privacy Policy (www.google.co.uk/policies/privacy/).

The College, as the domain administrator for Google's facilities, may have access to information held in an email account. The College reserves the right to access this information in the following circumstances:

- in connection with a criminal investigation;
- in connection with a properly authorised and evidenced investigation in relation to breaches or alleged breaches of the College's rules on use (including but not limited to whistleblowing, fraud and bribery);
- to meet legal or statutory requirements;
- in a situation (such as prolonged staff absence) where access is required to enable the College's business to continue; (Refer to page 3, point 7 about Delegate Access).
- in an emergency situation.

Where there is evidence of an offence, it will be investigated in accordance with the College's disciplinary procedures.

Confidentiality

Appropriateness & Attachments

Email, like any other form of communication, is not completely secure and its confidentiality cannot be guaranteed: messages can be intercepted by third parties, wrongly addressed, forwarded accidentally and forwarded by recipients to third parties. Before transmitting information of a confidential nature, users should assess whether it is appropriate to transmit the data in the email itself, or whether it should be in a document attached to/linked from the email. If documents containing sensitive information are sent from the College's network to external addresses, then staff must password protected and encrypt the attachments first.

For guidance on how to encrypt documents please review these websites links: https://www.groovypost.com/howto/geek-stuff/password-protect-encrypt-microsoft-office-2010- documents/

https://www.groovypost.com/howto/password-protect-encrypt-office-2016-documents-excel-word- powerpoint-o365/

Forwarding:

Before forwarding messages, whether externally or internally, staff should consider whether the authors of the messages would expect or be willing for this to happen. Staff should also consider whether the transmission of the information would breach the privacy of an individual or infringe copyright. In cases where it is necessary to send a message to a number of individuals – some (or all) of whom do not work for the College – care must be taken to prevent the recipients' email addresses from being disclosed

Transparency:

The **'BCC' facility** should be used to ensure that the addresses of the recipients cannot be viewed by each member of a distribution list.

Monitoring and record keeping:

Work-related emails are records of the College's actions and decisions, and must be managed as efficiently, and in the same way, as paper and other electronic records. There should be consistent, coherent controls in place to meet business and accountability needs, as well as to ensure legal compliance.

Messages must be checked regularly, prioritised and answered as promptly as possible. They should also be stored logically to ensure that information can be managed effectively and readily retrieved in response to enquiries (such as Data Protection and Freedom of Information requests).

Staff is encouraged to tag emails with Labels, Stars and importance tags to aid the management of current mail and retrieval of archived mail.

Access by Google:

Google also retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy

http://www.google.com/a/help/intl/en/admins/use_policy.html

Training and Guidance

Online training on the use of Google Mail and other G Suite applications are available at: https://gsuite.google.com/training/

Email Signatures

In order to present a consistent and professional image to those with whom the College corresponds, staff is expected to adhere to corporate guidelines when creating their email signature.

The logo used in the signature will be reviewed regularly and, where appropriate, updated to reflect those that most enhance our reputation. Staff will be informed when the logos to be used in the approved email signature change.

The format is as follows;

- Sign off
- Name | Role
- IBAT Logo
- Campus Address
- Contact details – Campus Main Switch, Direct Dial (if applicable), e-mail, website.

For example

Kind regards

John Doe | **Lecturer**

ibat DUBLIN
INSTITUTE OF BUSINESS AND TECHNOLOGY

16-19 Wellington Quay, Temple Bar, Dublin 2, Ireland

T +353 1 807 5055 DD +353 1 246 1508 E john.doe@ibat.ie W www.ibat.ie

Retention & Deletion

For further information please refer to Associated Policies 1.9, College Data Protection and Record Management Policy and 1.10 Data Retention Schedule that accompany the College Quality Assurance Handbook, 2021 V4.5

It is the responsibility of all staff to ensure that messages with continuing value are saved. Emails cannot be treated as a single series with a single retention period: the length of their retention must be determined by their subject matter or business purpose, as is the case with any other electronic or paper record.

Retention decisions should take into account business/operational needs, legal and regulatory requirements, accountability and transparency expectations. Messages relating to complaints, appeals, disputes and grievances should be retained as long as there is a need to preserve an audit trail.

The risk implications of deleting messages must be considered, as well as the obligation to comply with Data Protection legislation.

Google offers unlimited email storage, but this must not be abused. Staff is obliged to review their emails (both their inbox and their archived mail) on a regular basis to ensure that those that have served their purpose are deleted. Messages that are no longer needed should be moved to the Bin. Staff should be aware that all items placed in the Bin will be automatically deleted after thirty days and cannot be recovered. Whilst information is held in the Bin, it will be considered still accessible and may therefore have to be disclosed (in the period before erasure) in response to requests made under Freedom of Information or Data Protection legislation.

Shared email accounts

In departments where several staff are responsible for work activity and require access to the same emails, sharing access to a single account can make it easier to answer messages promptly and manage them effectively when individual members of the team are away.

Using a shared email delegated account should also simplify the process of sorting accounts when staff leaves: if team members keep the majority of their emails in a shared mailbox, less time should be required for reviewing individual accounts when staff leave the College.

Each shared delegated email account requires a primary contact that is responsible for the overall management of the mailbox, ensuring there are effective procedures in place for controlling incoming and outgoing messages.

Staff or departments can request temporary delegated shared access to email accounts. Staff requesting these types of account will be required to submit user information, rationale for account and expiration date to their Line Manager or Head of School (HoS)for approval. Following approval, a request can be logged with the IT Support Team: itsupport@ibat.ie

Staff should be aware that when they allow a colleague delegated shared access within Google Mail, they are granting full read and write access to that person. However, any emails sent from an email address using delegated permissions will need to be clearly identified as to the real author for each recipient.

Unless otherwise agreed between the user and their delegated colleague, access should only be used in times of absence or emergency. Anyone who is granted access to another user's account must respect the confidentiality of that account and must not view data that is clearly of a personal nature.

Absence from the College

In cases of planned absence, staff must set up an out-of-office message giving alternative contact details to ensure that enquiries can be answered promptly.

Illness or other unforeseen circumstances

In cases of illness or other unforeseen circumstances, where it is not possible to make any preparations for being away from the office, delegate access to your account will be through your line manager or the IT manager and not accessed by your peers.

The following actions are required by line management or HoS in the case of academic staff:

- Set up an automatic reply. To do this, the line manager or HoS should log a request with the IT Support Team, requesting that an auto-reply is added to the relevant staff account and supplying the exact text for the reply.
- Set up an auto-forwarding facility, if necessary. To request auto-forwarding, the line manager or HoS should similarly log a request with the IT Support Team: itsupport@ibat.ie
- Ensure emails received in the intervening period are dealt with, as necessary. If the line manager or HoS needs to gain access to the account to check whether there are business emails requiring attention, they should log a request with the IT Support Team: itsupport@ibat.ie

Leaving a department or the College

When members of staff leave the College, it is their responsibility to delete all personal messages and, in some instances, transfer access to appropriate colleagues.

Staff should be aware that, once they have left the College, they will no longer have access to their @ibat.ie email account, as this is the property of the College. It is therefore important that they remove all their personal emails – any items of a personal nature that they wish to retain should be forwarded to a private email address in advance of their departure.

It is also the responsibility of each staff member to ensure that an appropriate out-of-office response is set up to inform senders that they have left the organisation and give them alternative options for submitting their enquiry to another email address or department.

Expiration of Accounts

Staff and students may leave the College for a variety of reasons, which has implications on the duration of email privileges or when an account expires. The policy governing those privileges are set forth

below. Notwithstanding the guidelines below, the College reserves the right to revoke email privileges at any time.

- Staff members who leave the College will have email privileges removed effective on their last worked day. If such separation is for cause, email privileges may be immediately revoked without notice.
- Staff who have retired from the College will have email privileges removed effective on their last worked day.
- Students who leave the College without completion of their studies may keep their email privileges for one academic year from the last term when they were registered.
- Expelled students - If a student is expelled from the College, email privileges will be terminated immediately upon the directive of the Registrar's Office.
- Students who have graduated from the College will be permitted to retain their email account for a period of one year, follow which their account will be terminated.

DATA BACKUP & RECOVERY POLICY

BACKGROUND:

Backup strategy is one of the most important network services for the Staff & Lecturers. All corporate data, programs, databases etc. must be backed-up in accordance to the policy below and must be securely stored in a multiple devices local and remote for the purpose of archiving, recovery or restoration.

Objective:

- To safeguard the information assets of IBAT College Dublin.
- To prevent the loss of data in the case of an accidental deletion, system failure or disaster.
- To provide quick data recovery and restoration in a timely manner when urgent needs arises.
- To ensure that all historical archives are available to management in case of internal investigation, review or future reference.

Scope:

- This policy applies to all the Severs of IBAT College Dublin including NAS (Network Attached Storage) system and Swords Servers.
- Backups are stored in two different locations: Local (City Centre) and Remote (Swords).
- This policy covers user's stored information on their H: Drive or Home Folder from their Desktop and Laptop.
- VOICE data is not cover by this policy.

Data Backup

The following servers and data are the source of critical information that needs to be backed up based on the back up policy stated below on a regular basis.

SERVERS	DATA	NOTES
IBAT-SERVER7	WEB FILES	All webpages including databases
DATA-SERVER	STAFF FILES	All staff data, files and shared drives
WQ-DATA	Data backup	On site backup of data and VMs
Web-server	WEB FILES	New server to be migrated from Server7

WQ-PW1	PEARLWAY	Student Management System and RD app host
WQ-PROX1	DHCP, DNS, AD, Print	VM host for DC, student print and CoreDB server
WQ-PROX2	Secondary DHCP etc.	VM host for DC and staff print

Hardware and Media

Backups are stored in data servers operating high performance SAS hard drives in two different locations; one is in the Wellington Quay Campus and the other is in Frederick Street campus.

Internal Backup software

IBAT uses SynckBack Pro software to back up all our data and utilizes the entire backup options that we need. It supports a lot of features that meets the backup requirements of the college.

External Backup Solution

IBAT uses Google's Cloud Backup platform for daily incremental backups and archiving any new or modified files from a number of IBAT Servers. IBAT also conducts a weekly backup to external hard disks which are then disconnected from the IBAT network and stored security, this offers additional disaster recovery options, also ensures threats such as ransomware attacks cannot extend to these external backups.

Backup Schedules

Data is backed up according to the schedule below:

WQ-PW1 and Web-Server will backup dynamic data to their own dedicated backup drive B on a daily basis for quick restoration of accidentally deleted or corrupted data. This daily backup will also be copied to the dedicated backup server; WQ-Data.

A further weekly backup of more static data will also be copied to both Data-Server and WQ-Data. And off- site backup will feature a monthly full backup of all data

Each hyper visor has an archived image of all VMs it hosts as well as the other hyper visors in production. This allows for relatively seamless restoration of Domain Controllers, print servers, etc. in the event that virtual machines fail on the hyper visors themselves or if the physical servers failed, they can easily be rebuilt on new hardware. Copies of these archived VM images are also stored on data and backup servers.

Retention Policy

Pearlway, and TAS databases have a full daily (DAY 1 - 31) backup and a monthly backup which is retained permanently for archiving. For the Data File, has only a period of 3 days retention due to file size and storage limitation.

Verification

Syncback Pro performs full verification against a backup set after every job to protect against corrupted data. On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:

- To check for and correct errors
- To monitor the duration of the backup job
- To optimize backup performance where possible.

I.T. Services will identify problems and take corrective action to reduce any risks associated with failed backup.

Data Recovery and Restoration

In the event of an accidental deletion or corruption of information, requests for restoration of information will be made to the IT Services.

- ***Immediate restores***: Immediate restores are available to users via shadow copy, the Backup Server or form the Network Attached Storage.
- ***Restores from a particular day of the current month***: Only **Pearlway and TAS** are able to restore 30 days backward on a daily basis for the current month and can also be restored on a monthly basis. **Data File** can only be restored from 3 days backward. File versions beyond these days is not possible to recover.
- ***Restoration Request***: All restoration requests must be forwarded to IT Services Department via email. All the relevant information about the file or folder that needs to be restored should be written down in details i.e. filename folder name, date, version, type and other related information that will make the process quickly.

  IT Department is only liable to all the files that have been backed-up based on the policy stated above.

Local File Backup Policy

Background

Local Data Files are files that are IBAT College related information and mission critical data that are saved on your **Local Hard drive**.

What is a Local Hard Drive? A physical hard disk that is in your own PC where you save all the information on a specific folder such as "My Documents"

What is H Drive or Home Folder? This is a folder located on the network and not in your local hard drive. Home folder or Personal folder is part of the Z Drive Data File \ Users folder where you can save Corporate Data from your local hard drive to your own Home Folder.

Home folder is only accessible to the folder owner and cannot in any way be accessed by other staff.

A disaster can happen anytime such as Physical Error, Virus Infection, Natural or Environmental that will cause all your files to become accessible or possibly be deleted and become unrecoverable and unusable. Each staff has been provided with a Personal Folder on the network without limitation to be able to copy, backup or synchronize their data to and from.

Losing your data is disastrous, so regular backup is a must so that if disaster occurs, the IT Department are able to restore your data based on your latest backup.

Objective

- To ensure business continuity for all staff when disaster occurs.
- To provide information for all staff of the importance of regular back up.
- To be able to Backup and Restore Local Data Files when disaster strikes on staff Local PC or Laptop.
- To provide awareness for staff in terms of Data Protection and Security.

Policy

All Local Data Files that are ONLY related to company should be saved or backup to H Drive or HOME FOLDER on the File Server.

It is generally recommended that you store your most Corporate Data in your H Drive or Home Folder in the network.

Staff and Lecturers are given a personal storage on the network which should be used for storing and backing up company related files.

A simple copy and paste procedure is the only process for now to copy or back up your files from the "My Documents" folder to your H Drive or Home Folder.

Simple Copy and Paste Procedure

1. Make sure the file is **Closed**.
2. **Right click** the file on your local drive.
3. Choose **Copy** (nothing will happen after this.)
4. **Go** to your **H Drive or Home Folder** and choose a folder where to copy the file.
5. **Right click** the correct folder destination and choose **Paste.** Please see policy no. D11 for Overwriting Files.
6. You can also copy a whole folder but be careful on the overwriting process.

User Responsibility

It is the responsibility of all staff to keep his or her Local Files to be backed up regularly in the H Drive or Home Folder.

- It is the responsibility of all staff to back up ONLY company related data and not personal data.
- It is the responsibility of all staff to protect and secure their Local Data File stored on their Local Hard Drive
- IT Department DO NOT recommends backing up Corporate Data in an external storage or USB stick without permission from the IT Department for security reasons.

IT Department and Exceptions

- Special software will audit file access and back up time for each staff in order to monitor the time and date of your last backup so that we can restore whatever latest information based on the audit and in your last backup.
- IT Department is responsible for backing up all Corporate Data saved on the Z Drive including staff Home Folder.
- IT Department is responsible for keeping the Corporate Data secure and should be backed up regularly in accordance to the Network Backup Policy.
- IT Department will NOT be held liable for any loss, deleted, corrupted data on your local drive if this policy has not been followed accordingly.
- IT Department is NOT responsible for accidental OVERWRITING with your existing files on the H Drive or Home Folder. Please ensure that before deciding whether you will overwrite the file/s & folder/s or not, please review the changes first and the target document itself.
- Windows Systems detects if the file you are copying already exists on the destination. A confirmation will pop up on the screen that will compare the file that you are copying and the file already there, and this gives you the decision if you want to overwrite it or not.
- Windows will give you detailed comparison of the file size, date and time of modification etc. So you must be aware of these details. Overwritten files are irreversible.
- IT Department treats every single document as highly classified information and should not be opened and read, sent out by email or distributed without proper authorization from senior management.

- IBAT College Dublin reserves the right to review and or require change of any identification and/or authentication process for compliance with this policy.

Anti-Virus

All servers are protected by AVG Antivirus Internet Security Business Edition. All servers are scheduled to scan on a daily basis.

Wireless Access points

All Cisco Wireless Access Points across the college supports the following security encryption:

- **Wireless Personal Access:** that uses TKIP Cipher Suite
- **Wireless Personal Access 2;** that uses CCMP (AES) Suite to provide additional security.
- **SSID ID** is broadcast to make it available for the students
- **Encyption Key** is 11 character combinations of numbers and letters.

Firewall

- IBAT FIREWALL USES ONLY 3 PORTS TO ALLOW ACCESS ON THE INTERNAL NETWORK.
  - 80 FOR WEB
  - 443 FOR SSL
  - 139 FOR RDP
- IBAT Firewall is not part of the Internal LAN subnet and uses different IP for security reason
- IBAT Firewall web management interface is encrypted and password protected.
- IBAT Firewall is up to date to the latest firmware as possible.

AP1.20 IBAT College Dublin IT Password Policy V1.3

Contents

Purpose

The purpose of this document is to provide specific guidance to users and IT administrators in TechnologicalUniversity Dublin (hereafter referred to as "IBAT College" or "the College") on the use of **passwords** (also known as **passphrases**) to access University on-line resources. This is because passwords/passphrases are animportant aspect of information security, and a poorly chosen password could result in IBAT College data being lost or stolen. All users, including 3rd-party contractors and visitors with access to the College's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Definitions

Dictionary Attack: A method of breaking into a user's account by systematically entering every word in adictionary as a password

Encryption: The encoding of data so that it cannot be read without the correct decryption key

Mobile Device: These can include, but are not limited to:

- Smartphones (e.g. iPhones, Android phones)
- Tablets (e.g. iPads, Kindle Fire, Android tablets)
- Portable storage devices such as USB memory sticks, removable hard drives, etc.

Password: A password is a sequence of words or other text used to control access to a computer device,application or data. A passphrase is similar to a password in usage, but is longer, and less reliant on complex characters, making it easier to remember.

Single Factor Authentication: A process for validating a digital identity using only one set of credentials(e.g. password), in order to gain access to a resource, such as a computer or application

Multi Factor Authentication: A process for validating a digital identity using more than one factor (e.g. a password together with a digital token sent to a mobile phone or physical device/token), in order to gain access to a resource, such as a computer or application.

Roles and Responsibilities

The following roles and responsibilities apply in relation to this policy where appropriate:

IT Department:

- To clearly communicate information to users on how to create and change secure passwords
- To Liaise with the Office of the College Secretary and/or The College Compliance Group on information received in relation to potential breaches of the policy
- To enforce compliance with this policy where technically possible on IBAT College systems
- To provide tools such as a password-strength meter, or blacklisted words to assist users in choosing

a secure password

- Where not technically possible to enforce this policy, to apply the Information Security Exception policy, and in the interim to instruct end users to create appropriate passwords
- To regularly review the list of accounts with access to business data, and to ensure access is revoked where staff exit their role
- Review the password policy, and where appropriate, liaise with IT Services for the configuration of additional security measures

Staff / students / Third Parties:

- To adhere to the practices contained in this document.
- To report suspected breaches of policy to the relevant IT Service Desk.

If you have any queries on the contents of this policy, please contact the Head of IT Services for yourcampus.

Scope

This standard applies to all users who are allocated an account (or any form of access that supports or requires a password) on any system that has access to the IBAT College network, stores any personal data or private non-personal IBAT College data, or has been authorised as a IBAT College service including, but not limited to, external cloud services.

Password and Standards

General Standards

- The user is the sole custodian of the password, and must protect the password at all times
- IBAT College user account passwords must never be transmitted over the telephone or IT network (e.g. email) in a clear text format
- Passwords must be protected at all times, and measures must be taken to prevent disclosure to any unauthorized person or entity
- Passwords can be changed using the College's self-service tools. Passwords will only be manually reset by the IT Service Desk when the identity of the user can be verified in person.
- Password must not be written down or stored digitally, unless appropriate security measures are in place (e.g. physical security, strong encryption)
- Passwords must not be shared and ICT services will never ask you to divulge your password.
- Passwords used for IBAT College accounts should not be used with non-IBAT College systems (e.g. LinkedIn, Twitter), even for work-related purposes
- Passwords must be changed immediately when:
    - The password is a default or temporary token created by someone other than the user.
    - A new system is deployed with default vendor passwords
    - The password is suspected to have been shared or compromised

Password Requirements

It should be noted that the requirements outlined in this section should be considered the minimum levelof password security that should be applied to IBAT College passwords.

1. All passwords must be a minimum of 8 characters in length, and contain from at least three of thefollowing four character classes:
    - Upper case alphabetic (e.g. A-Z)
    - Lower case alphabetic (e.g. a-z)
    - Numeric (e.g. 0-9)
    - Special characters (e.g.

    .,!@#$%~)Password **must not**

    contain:

    - Any words with simple obfuscation (for example: p@ssw0rd, g0ldf1sh, etc.);
    - Any personal information related to a user - (for example: user name, address, date of birth,staff/Student number, car registration number, telephone number);
    - sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);

2. The expiration period for passwords must be set to a maximum of 180 days.
3. The minimum password age must be set to at least 1 day.
4. The password history setting must be set to remember at least the last 10 passwords.
5. After 10 failed login attempts an account must automatically be disabled for at least 5 minutes or untilit is reset by a system administrator.
6. The initial password issued must be set to expire at first login, requiring the user choose anotherpassword before continuing the login process.
7. Multi factor authentication will be enforced for off-campus access to IBAT College systems and data
8. Staff performing administrative tasks with elevated privileges must use a separate account for thispurpose. The username for such accounts should clearly identify the assigned user.

AP1.21 IBAT College Dublin Attendance, Punctuality & Engagement Policy

Document Title and Reference	IBAT College Dublin Attendance, Punctuality & Engagement Policy
Purpose	The source of reference for the policies, procedures, principles and practices upon which IBAT College Dublin quality assurance mechanisms are based.
Version	V1
Author/Proposed/endorsed by	Registrar
Approved by	Academic Council
Approval date	November 23rd 2023
Endorsed by	Board of Governors - December 5th, 2023.
Effective from	January 2024
Review date	March 2026 (Reviewed March 2025)

Introduction

Studies show that attendance, punctuality, and engagement are important determinants in successful academic achievement. In addition, the benefits of maintaining high standards in such matters create a quality learning environment for all participants. Poor attendance, punctuality and engagement impacts on the dynamic in the class, progression between stages and in some cases can lead to withdrawal from a programme (voluntary and involuntary means).

Attendance Monitoring in IBAT College Dublin is conducted in all three schools, English Language, Higher Education and Professional Diplomas. The student management systems are updated on a weekly basis. This is particularly important for international students who are resident in Ireland on a student visa and are required to study full time (minimum 15 hours per week) and to maintain an attendance level of a minimum of 85% in all classes. IBAT College Dublin is required by the GNIB (Garda National Immigration Bureau) to monitor student attendance and to report to the GNIB any student whose attendance is below this threshold.

Attendance data informs decision making in the college and meets the college's statutory obligations under visa regulations and other third-party data requests, e.g., state agencies and bodies such as HEA, An Garda Siochana etc. All data sharing and retention is in accordance with GDPR regulations.

Punctuality & Attendance Policy

Ideally you arrive 15 minutes in advance of your lecture to ensure the full timetabled lecture is devoted to learning and not housekeeping matters.

Lecturers are required to complete an attendance sheet for each class, at the beginning of that class, leaving no incomplete fields. Absence after a break is noted. This information is recorded and used to calculate attendance statistics.

Students who arrive more than 15 minutes late for class may not be permitted to enter the class until after the break and will be marked absent for that block. Latecomers can be disruptive for the lecturer and their peers. Any lateness and/or non-attendance will be noted on the appropriate sheet. Students can check their own attendance online on a weekly basis in the Moodle system accessible through their personal student profile. They are also free to verify this at reception or by contacting their student Academic Administrator.

It is the student's responsibility to provide documentary evidence (e.g., medical certificates, hospital appointments etc.) to support absences from class. Such documentation must be copied for filing purposes and/or appropriate authorities. It will be held securely in line with Data Protection requirements.

How non-attendance is handled

If a student is repeatedly not attending class, they will first be given a preliminary warning by email (Warning 1). If there is no improvement in attendance and/or requirements are not being met, a further email (Warning 2) is sent to advise students of the situation. Failure to respond to either of these results in students being advised by email (Warning 3) to attend a meeting (one week later) with the Head of School, Programme Administrator and Student Affairs Coordinator to discuss the situation.

Academic and pastoral support will be invoked, where appropriate to allay student concerns, such as personal mitigating circumstances (Refer to QAH Section 8.8.2 Mitigating Circumstances).

Following this meeting, if there is continued non-compliance regarding attendance, students will be emailed formally by the Office of the Registrar to advise them that the Garda National Immigration Bureau have been notified of their attendance to date. In this instance, an exit letter will be sent to the GNIB.

Process is outlined as:

- **Warning 1** (if attendance falls below 85%)

  ↓ (3 weeks)

- **Warning 2**

  ↓ (3 weeks)

- **Warning 3** (the student is asked to attend a meeting)

  ↓ (3 weeks)

  Meeting with Head of School, Programme Administrator and Student Affairs Coordinator (written agreement to attend ALL classes)

  ↓

  Expulsion (if another class is missed, a letter is sent by the Office of the Registrar to GNIB and Operating Protocol & Procedure 3.3 - Protocol on the College expelling a Student is invoked)

Non-Engagement

Even if a learner has not attempted the maximum number of opportunities to pass a module, a learner can be presented to an Exam Board with a recommendation to withdraw because they failed to adequately engage in the assessment components of a programme. This is as a result of one or more of the following happening:

- non-submission of more than 50% of assessment components for that stage.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

- non-participation in more than 50% of assessment components for that stage.
- Repeated failure to communicate with the college, within a reasonable period, in relation to extremely poor academic performance.

It is the learner's responsibility to be fully aware of the impact (both on their marks and subsequent award classification) of failing to submit or failing to pass assessment components. In addition, in the case of suspension and expulsion the learner must be aware of the following financial implications:

- *Suspension –*

  (i) if in the current academic year, any fees paid for the semester are forfeited.

  (ii) Future semester – if suspension still applies in this period fees are not refunded BUT are applicable to the next academic year when the suspension ceases.

- *Expulsion –*

  Any fees paid are non-refundable.

Appeal the decision.

Disagreement with the decision does not constitute grounds for appeal. Section 7.16.7 outlines the operation of the Appeals Board. Please note the grounds on which an appeal will be considered. The Appeals Board is not a new hearing or new investigation does not occur. The role of the Appeal Board is to re-examine the procedure and/or decision made in determining suspension / expulsion.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

AP1.22 IBAT College Dublin Artificial Intelligence Policy

IBAT College Dublin Artificial Intelligence (AI) Policy

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

Artificial Intelligence (AI) Policy - IBAT College Dublin

Title	Artificial Intelligence (AI) Policy V1 - IBAT College Dublin
Effective Date	March 20th 2025
Associated Policy	AP1.22
Owner	Registrar
Updated By	Registrar / Dean
Reviewed By	Dean, Registrar, Director of IT, Managing Director, Programme Team, Lecturers
Approved By	Academic Council – 20th March 2025
Related Policies	Quality Assurance Handbook Section 8.16 Academic Misconduct
Related Forms	F8.5 Academic Misconduct Form
Version History	NEW Policy – Mar 2025 (V1)

1. Purpose

This policy establishes guidelines for the ethical and responsible use of Artificial Intelligence (AI) at IBAT College Dublin.

AI has changed the landscape of higher education (HE), offering transformational ways in how we acquire knowledge whilst simultaneously creating challenges in assessment integrity. QQI states that.

> *GenAI has potentially wide-ranging implications for their operations, including the appropriateness of curricula and approaches to teaching, learning & assessment; quality assurance arrangements; policy and procedure; engagement with and responsiveness to disciplinary and industry developments; staff recruitment and development; and technological and legal infrastructure.*
>
> *https://www.qqi.ie/news/artificial-intelligence-snapshot#:~:text=For%20providers%20of%20education%20and,and%20responsiveness%20to%20disciplinary%20and*

This policy aims to support innovation, academic integrity, and operational efficiency while mitigating risks associated with the use of AI technologies.

This policy has been informed by our membership in the National Academic Integrity Network, review of AI policies in other colleges, a review of literature in this space, etc.

2. Scope

This policy applies to all lecturers, learners, staff, and third-party vendors using AI within the college environment. It covers academic, administrative, and research applications of AI, including AI-generated content, decision-making, and automation tools.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

3. Guiding Principles

- **Ethical Use:** AI must be used in ways that align with the college's values, including integrity, collaboration, and empowerment. Fairness, transparency and accountability will guide any use of AI.
- **Academic Integrity:** AI tools must not be used for academic dishonesty, such as plagiarism or unauthorized assistance in coursework. The college expects that all work from a learner for grading purposes is original and their own. Academic integrity is an essential aspect of consideration prior to submission of any assessment to the college. Guidance will be provided to all learners on the appropriate use of AI, what happens when there is a suspected infringement of academic integrity, and the appeals process thereafter.
- **Data Privacy:** AI applications must comply with data protection regulations to safeguard personal and institutional information.
- **Human Oversight:** AI should complement NOT replace human judgement in the decision-making process.
- **Accessibility and Inclusivity:** AI must be deployed in ways that promote equal access to educational resources and avoid bias.

4. AI in Academics

- **Use by learners:** Disclosure of the use of AI tools in assignments, projects, or research as per assessment guidelines provided by your lecturers.
- **Use by lecturers:** You must clearly communicate whether AI tools are permitted or restricted in coursework and assessments.
- **Plagiarism and Misuse:** Unauthorized use of AI for generating assignments, research papers, or exam responses will be considered academic misconduct and the process as outlined under section 8.16 in the College Quality Assurance Handbook will be invoked.
- **AI-Assisted Learning:** AI tools can be used to enhance learning experiences, provided their use is transparent and approved by lecturers.

5. AI in Administration

- **AI for Decision-Making:** AI may be used to support administrative decisions but must not be the sole determinant.
- **Employee Responsibilities:** Staff members using AI for work-related tasks must ensure accuracy, fairness, and compliance with institutional policies.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

- **Third-Party AI Services:** Vendors providing AI solutions must adhere to ethical AI practices and data security standards.

6. Research

ATU Learners - Refer to ATU Ethical Guidelines, contained in the Student Handbook for your course of study.

7. IBAT Learners on QQI programmes

Research is a skill acquired during your studies in the college. When research is being conducted, please ensure the research approved prior to commencement, if applicable. In addition, that it is conducted ethically, risk assessment is conducted, informed consent and confidentiality matters have been considered. Guidelines will be provided.

8. Data Privacy and Security

- **Compliance:** All AI applications must adhere to relevant data protection laws (e.g., GDPR) and institutional policies, e.g. Associated Policy 1.9 - College Data Protection and Record Management Policy.
- **Data Minimization:** AI systems should collect only the necessary data to perform intended functions.
- **Security Measures:** Appropriate security protocols must be in place to prevent unauthorized access and data breaches.

9. Monitoring and Review

- **Policy Compliance:** Violations of this policy may result in disciplinary actions, including academic penalties, employment sanctions, or revocation of access to AI tools.
- **Periodic Review:** This policy will be reviewed annually to reflect technological advancements and emerging ethical considerations.
- **Feedback Mechanism:** Lecturers, staff, and learners are encouraged to provide feedback on AI usage and its impact within the college.

10. G. Contact Information

For questions or clarifications regarding this policy, please contact Office of the Registrar at registrar@ibat.ie.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

Resources:

1. Using GenAI in Teaching, Learning and Assessment in Irish Universities - Examples from the Disciplines

   Authors: Dr Ana Elena Schalk Quintanar (Editor) and Dr Pauline Rooney (Editor)
   https://ucclibrary.pressbooks.pub/genai/

2. Generative Artificial Intelligence: Guidelines for Educators, National Academic Integrity Network

   https://www.qqi.ie/sites/default/files/2023-09/NAIN%20Generative%20AI%20Guidelines%20for%20Educators%202023.pdf

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

AP1.23 IBAT College Dublin Learner Assessment Feedback Policy

IBAT College Dublin Learner Assessment Feedback Policy

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

Title	Learner Assessment Feedback Policy
Effective Date	20th March 2025
Owner	Dean
Implemented by	Programme Leader, Programme Manager
Approved by	Academic Council
Review Date	March 2026

Overview

At the Institute of Business and Technology (IBAT) College, Dublin, we recognise that assessment feedback is a fundamental part of the learning process. Effective feedback helps students understand their strengths, areas for improvement and develops the skills necessary for academic and professional services. This policy outlines our commitment to providing timely, constructive and meaningful feedback that enhances student learning and engagement.

Our approach to assessment feedback is guided by principles of clarity, fairness and accessibility. We aim to ensure that all students receive feedback that is specific, actionable and supportive of their academic progress, in addition to the grade achieved. This policy applies to all forms of assessment across all our programmes and is designed to foster a culture of continuous improvement and reflective learning.

By setting clear expectations for lecturers and academic staff, this policy ensures that feedback is not only a tool for evaluation but also a catalyst for growth, promoting deeper learning and a more enriching educational experience at IBAT College.

It is the intention of this policy to confirm to students their entitlement to assessment feedback and to provide academics with clarification on their obligations in respect of providing feedback to learners.

Course Assignments

Where possible lecturers should endeavour to provide feedback to students in a timely manner and ideally within 14 days of the submission date. Exceptions apply in respect of late submissions.

All assessments must be supplied with assessment criteria and a marking scheme. It is expected that feedback to learners will be provided by lecturers online using via Moodle, using the assessment criteria as a framework for feedback.

IBAT College Dublin 16-19 Wellington Quay,
Temple Bar,
Dublin 2, Ireland
Tel: +353 (0) 1 8075055
www.ibat.ie

Feedback must be in a format that enables learners to revisit the feedback at a later date, should they wish to do so. Effective feedback should be clear, constructive and aligned with learning outcomes, ensuring that students understand their performance
and areas for improvement. The following characteristics define high-quality summative feedback on course assignments:

Clarity and precision: Feedback should be specific, concise and easy to understand. Feedback should directly reference assessment criteria, highlighting where students have met expectations and where they need further development. Feedback should be constrictive and help the student to understand where their work can be improved.
Feedback should be unambiguous, so it is clear to any moderator or external examiner as well as the student, what the assessor's view are and why.

Alignment with learning outcomes: Effective feedback should be directly linked to the intended learning objectives of the assignment, reinforcing key skills and knowledge
required for academic success.

Balanced and constructive: While acknowledging areas for improvement, feedback should also highlight strengths. A balanced approach encourages student motivation and helps them build confidence in their abilities.

Actionable guidance: Feedback should provide clear suggestions for improvement, offering students practical steps they can take to enhance their future work. This
ensures that feedback is not just evaluative but also developmental.

Timelines: The most effective summative feedback should be provided promptly, allowing students to reflect on their performance and apply insights to subsequent
assignments. Delays in feedback can reduce the impact of the feedback on learning.

Consistency and fairness: Feedback should be standardised across courses and lecturers, ensuring that all students receive equitable and objective evaluations.
Consistent use of grading rubrics and assessment criteria helps ensure fairness. While assessment is an informed professional judgement, it is a judgement against specified learning outcomes in relation to a specific activity. Terminology expressed in the
feedback should be reflective of the mark awarded.

Group assessment feedback: Group assessment feedback should be clear, balanced and based on individual and collective contributions, using structured criteria to ensure fairness and actionable improvement.

Encouragement and reflection: High-quality summative feedback should encourage students to engage in self-reflection, helping them critically assess their own work and develop independent learning strategies.

By incorporating these characteristics, summative feedback becomes a valuable tool not only for assessing student achievement but also for fostering continuous improvement and deeper learning.

Format of feedback: feedback may be automated, provided in written, audio, video format or verbally. Sample answers may be provided, but this is not a requirement, nor is it relevant for every assessment.

Feedback on examination performance and discussion of scripts

As per QQI Assessment and Standards (2022), students at IBAT College have the opportunity to seek feedback on their examination performance and discuss their examination script. Students are advised that discussion of examination scripts is intended as a feedback process to assist understanding and enhance future examination performance. Students who wish to appeal their examination result should follow the IBAT Appeals procedure.

AP1.24 IBAT College Dublin Alumni Policy

Alumni Policy V1 - IBAT College Dublin

Title	Alumni Policy V1 - IBAT College Dublin
Effective Date	20th March 2025
Associated Policy	AP1.24
Owner	Registrar
Updated By	Dean & Registrar
Reviewed By	Dean, Registrar, Director of IT, Managing Director, Programme Team, Lecturers
Approved By	Academic Council
Related Policies	Quality Assurance Handbook Induction and Feedback policies.
Related Forms	First Destination Survey
Version History	NEW Policy – March 2025 (V1)

1. Purpose

A strong connection with graduates provides the opportunity to connect with graduates of the College, mainly through email, social media contact, and any graduate/industry engagement events as appropriate.

The College seeks to continue the relationship with and between graduates. Ongoing networking between alumni and currently enrolled learners, the College, and external stakeholders such as the Expert Advisory Panel, is vital to the ongoing personal and professional development of learners and graduates of IBAT College Dublin.

The Student Affairs Coordinator is the primary point of contact for alumni.

A graduate is a former learner of the College who has graduated from a programme of study delivered in the College. The status of alumni is automatic for those who have pursued and completed academic programmes leading to graduation.

In respect of Professional Diploma courses a minimum of 3 months in duration is required.

Graduate surveys are distributed to recent graduates at graduation and/or between six to nine weeks after they graduate. Graduate feedback is collated and analysed by the School for the purpose of feedback and statistical and profiling analysis and may be communicated and shared with programme leaders, the Senior Management Group and Academic Council on an aggregate basis only. This information is used to inform, for example, future events, programme developments, and learner service enhancements and may be used in aggregate to communicate example outcomes and chosen fields for graduates of current programmes.
All contact with graduates will be GDPR compliant and on a permission-based basis.

2. Standard Operating Procedures

SOP 2.1 Evaluating an Application for Entry to an Academic Programme

INTRODUCTION AND SCOPE

This Standard Operating Procedure (SOP)

- is to be used for all admissions to academic programmes at IBAT College Dublin.
- supports IBAT College Dublin's Admissions Policy and sits under the College's QAH 2018
- defines the terms used in the IBAT College Dublin admissions policy (see section 5 below).
- does NOT cover advanced entry or exemptions.

There is considerable overlap between admissions and recruitment and it is usually the recruiter who is in contact with the applicant. However, the responsibility for the admissions decision lies with the Registrar. The role of the Admissions Officer (currently incorporated within the Registrar's Office) is to recommend an admissions decision, which will be endorsed by Head of School and ultimately underwritten by the Registrar.

The responsibility for recommending admissions decisions via Recognition of Prior Learning (RPL) lies with the Head of School and is underwritten by the Registrar.

The Registrar is supported by the Admissions Committee in ensuring that the admissions process is robust and that all admissions decisions are correct, are properly recorded, that files are audited and are accessible for review.

PROCEDURES

The documents required to evaluate an application include:

- Complete application pack
- Copy of the programme entry requirements
- This SOP
- Access to NARIC Ireland to evaluate the qualification(s) of the applicant
- Access to UK NARIC to determine if the awarding body is recognised
- A copy of the IBAT College Dublin recognised English Language qualifications
- The IBAT College Dublin Application Form has been laid out to ensure collection of all required applicant information, and includes an applicant summary sheet. This summary sheet must be completed by the recruitment team BEFORE an evaluation can be undertaken.

EVALUATION

The purpose of the evaluation is to determine if (i) the application meets the programme entry requirements specified at validation, and (ii) if the candidate has a reasonable chance of meeting the minimum intended programme learning outcomes.

<u>Evaluating Applicant Details</u>

- <u>For Standard Entry</u>

  Applicants should complete ALL sections of the relevant application form.
  In addition postgraduate applicants should supply a simple CV listing all academic institutions attended, academic qualifications and work experience (noting if FT or PT) in chronological order. A 300 word statement of purpose is preferred but not essential.

- <u>For Non-Standard Entry</u>

Applicants will need to complete additional information depending on the route to entry, mature (UG only) or RPL. To evaluate an RPL for entry to an academic programme the applicant will be required to submit additional material as laid out in Section 3.4.1, below.

The applicant details and the applicant summary sheet must be completed, by the recruitment team, before the evaluation progresses. This completed applicant summary sheet, and the full application pack, is forwarded to the Registrar's Office.

Evaluating an Admission

When evaluating an application the evaluator is looking for evidence of sustained academic achievement and commitment to the programme of study. A series of poor or failed transcripts may indicate future poor performance. In these cases a record of attendance from the former college may be requested.

Applicants who will need to avail of the Reasonable Accommodation Policy should be identified as early as possible so their needs can be evaluated and can be met by the College. All applicants citing needs should include appropriate documentary evidence such as a current and recognised educational psychologist's evaluation. Student Affairs should be notified of all successful applicants who have specified needs under the policy for Reasonable Accommodation. For further see the Policy for Reasonable Accommodation (**Section 8.8 QAH 2018**).

Evaluating Academic Credentials

Applicants must supply certified (or original) copies of all academic transcripts - all admission decisions are conditional on the authenticity of transcripts.

The recruitment team check that the academic qualification is (i) recognised, (ii) is at the NFQ level specified in the entry qualification, and (iii) the candidate has achieved the required grade.

(i) The awarding body, university or college is checked on UK NARIC (https://www.naric.org.uk/naric/login.aspx) and a printout is added to the pack
(ii) The award is checked on NARIC Ireland to establish its comparable level on the NFQ. The comparability statement is downloaded and added to the pack. (http://qsearch.qqi.ie/WebPart/Search?searchtype=recognitions)
(iii) The grade achieved must match that specified in the entry criteria. In some cases a comparison must be judged. World Education Services may support this judgement. (https://applications.wes.org/country-resources/)

The application is passed to the Registrar's Office who may further verify the academic credentials and determines who should carry out the RPL consideration, usually Head of School or delegate. The Registrar's Office logs the application for reporting purposes and forwards the application pack with the decision deadline to the Head of School or delegate – the decision deadline usually within 48 hours of receiving the complete pack from recruitment.

If a candidate has not achieved the required academic qualification for the programme their application may be considered under the Colleges policy for RPL for Entry. See section 3.4.

English Language Requirements

ALL candidates are assessed for English Language regardless of citizenship.

Candidates automatically qualify if:

- They are a citizen of, and were formally educated in, a country where English is a majority language and is listed in ***Reference 3***.
- they have successfully undertaken, in the last five years, a recognised academic programme of not less than 60 ECTS listed in ***Reference 1 and 2*** for QQI awards or ***Reference 3*** for UWTSD awards.

NOTE:

All IELTS (academic) transcripts are verified *via* *https://www.ielts.org/ielts-for-organisations/processing-and-verifying-ielts-results* and are deemed current if taken within the last 2 years (24 months).
In all other cases candidates must produce evidence that they have attained the level of English specified in the entry qualifications for the programme.

Recognition of Prior Learning for Entry

A candidate being assessed *via* an RPL for entry may have a portfolio comprising all three elements of RPL

- RPL Formal - a formal framework qualification, albeit not at the level or grade required in the entry requirements.
- RPL Non-formal - professional or non-framework diplomas, such as an IBAT College Dublin Diploma.
- RPL Informal - experiential learning that takes place through life and work experience. Often it is learning that is unintentional and the learner may not recognise at the time of the experience that it contributed to his or her knowledge, skills and competence.

The role of the evaluator, normally Head of School or delegate, is to establish if the portfolio of learning has taken the applicant to the level required by the programme entry requirements in terms of knowledge, know-how, skill and competence.

Material Required for RPL Portfolio

Candidates applying under RPL for entry should include:

1. A CV including
   a. all qualifications, awarding bodies, levels, credits and grades in chronological order.
   b. all courses, certificates or other non-formal learning completed
   c. all evidence of employment, in chronological order, specifying whether fulltime or part-time with duration of contract, duties and responsibilities.
2. A letter from employers endorsing the applicant's work, or the contact details and permission to contact for reference/verification
3. A letter or statement outlining their rationale for/commitment to undertaking the course and why they believe they are prepared to undertake the programme at this time.

Evaluating a portfolio for RPL

The evaluation of a portfolio is a review of the applicant's level and volume of learning and work experience to establish if they have attained a level equivalent to that specified in the programme entry requirements. This evaluation requires a large element of judgement and therefore is carried out by an experienced academic nominated by the Head of School.

Level – Evaluate the candidate's identified previous responsibilities and achievements against the relevant Level Indicators (**Reference *4***). For example at Level 8 competence would imply the ability to '*to act effectively under guidance in a peer relationship with qualified practitioners; lead multiple complex and heterogeneous groups'* or to be able to *demonstrate exercising appropriate judgement in planning* etc. This must be endorsed by an employer/referee.

Volume - Ensure that any employment is continuous, is listed in chronological order, and has been fulltime (usually fulltime role for at least two years is required for consideration). This must be supported by a reference.

The portfolio evaluator may call the applicant for interview, will record their evaluation and rationale for admission or rejection, and include their notes and decision with the applicant file.

MAKING AND RECORDING AN ADMISSIONS DECISION

The Registrar is responsible for ensuring the policies and procedures for admissions are fit for purpose and implemented.

On completion of the evaluation the Head of School or delegate makes a recommendation to the Registrar.

All admissions decisions are signed-off/approved by the Head of School, the Registrar.

The Registrar or nominee (which can include the Head of School) signs the applicant's form, includes the rationale for the decision, and identifies any conditions (where the offer is conditional) and returns the form to the Registrar's Office who logs the decision and passes on to the Recruitment team to communicate the offer.

All Non-Standard applications are subject to audit and review by the Admissions Committee.

All RPL decisions are reviewed by the Admissions Committee and the applicants academic outcome, at the end of the programme, is recorded for programme monitoring and review purposes.

GLOSSARY

Advanced Entry – Applicants who wish to access a programme at a stage other than stage 1. See IBAT College Dublin Policy for RPL.

Exemptions – applicants who wish to be exempt from a module or modules at any stage of the programme. See IBAT College Dublin policy for RPL.

Non-Standard Entry/Applicant – applicants who do not, at first evaluation, satisfy the entrance requirements for entry into stage 1 of an academic programme, and who wish to be evaluated by RPL or are classified as mature entry.

Recognition of Prior Learning (RPL) – this includes formal and non-formal (certified) and informal (experiential) learning and is described in the IBAT College Dublin policies for RPL. RPL can be used for admission, advanced entry, or exemptions.

Standard Entry/Standard Applicant – applicants who satisfy the entrance requirements for entry into stage 1 of an academic programme.

REFERENCES

1. Agreed entry requirements criteria for EU/EFTA Applicants for 2018 entry – Thea, IUA and RCSI
2. AP 1.3a IBAT College Dublin English Language Recognised Equivalence
3. AP 1.3b UWTSD English Language Entry Requirements for Academic Study – Including Countries where it is recognised as English speaking for the purposes of entry to UWTSD
4. QQI Grid of Level Indicators

SOP 2.2 Nomination Procedure for Staff and Learner Representatives to the Board of Governors

- One current learner nominated by the student body and co-opted*
- One member of College staff co-opted by the Board.

Tenure – one year, renewable, determined by Board of Directors. *From QAH V4.3*
The Registrar's Office manages this process.

Process:

1 Staff Representative

A call for nominations is made to each department by the Registrar's Office in October of each year. The call is accompanied by a copy of this process and the Terms of Reference:

Table 1 - Departments:	**Nominated by:**
Finance and Facilities	CFO & Head of Facilities
Marketing and Recruitment	Marketing Manager & Recruitment Manager
Registry	Registrar
Higher Education Team	College Principal
Business School Academics	Head of School
School of English – Admin and Management Team	College Principal
School of English - Teachers	Director of Studies WQ & Director of Studies NFS

On receiving the call each department head will provide an opportunity for staff to volunteer. Where more than one staff member volunteers the department head or managers (See Table 1 above) will select the nominee based on a transparent criterion such as a defined performance metric, or demonstrable capabilities.

The nominated staff member will be required to supply a short biography (see template below).

The Registrar sends the list to the Chair of the Nominations Sub- Committee who will select a candidate to be co-opted to the Board.

2 Learner Representatives

On election by the class, all class representatives will be asked if they are interested in running for Board of Governors. Those interested submit a biography, see template below, to the appropriate Programme Administration Manager. A recommendation will be made by the Head of School in consultation with the school and all nominations forwarded to the nominations committee with the recommendation of the HoS. The length of the nominees programme (tenure with the college) should be taken into account.

Name, Job Title

Years at IBAT, About me (two lines), What would my seat at the BoG mean for learners at IBAT?

SOP 2.3 Procedures for Registration to a Programme at IBAT College

1. INTRODUCTION AND SCOPE

This Standard Operating Procedure (SOP) supports section 5.10 the policy on Registration of Learners in the QAH and applies to the registration of ALL learners to ALL programmes at IBAT College Dublin.

Registration is required before anyone can attend scheduled classes.

Eligibility criteria may vary with the status of the programme, however the absolute minimum level of information required, includes proof of:

- Identity
- Age
- Nationality and/or residency
- PPSN OR Passport Number
- One form of contact e.g. address or email address.

The responsibility for the registration process lies with the Registrar. The responsibility for ensuring that all documentation is presented for authentication is with the applicant.

2. PROCEDURES

An applicant may be registered with the College once they have fulfilled ALL of the following conditions:

- Received an unconditional offer to an IBAT programme
- Signed an offer acceptance form (for academic programmes)
- Signed up to the College Terms and Conditions
- Paid fees or agreed payment plan as agreed with the College
- Set at 'eligible to register' status on the LMS.

When the applicant is deemed eligible to register the registration process includes checks on the following information:

- Personal details including passport and visa, where appropriate
- Permanent Address
- Term Address
- Contact details
- Contact details for next of kin

The following documents are subject to verification:

- Passport including visa where appropriate
- Originals of academic transcripts and proof of English Language, where appropriate
- Proof of address

3. REGISTRATION PROCESS

The registration process is organised by the Registrar's Office and precedes Induction which is the responsibility of the school.

The process includes:

- Uploading photograph
- Verification of documentation (see section 2 above)
- Receipt of Student Card and email address
- Receipt of Timetable and Student Handbook

- Signing up to Student Code of Conduct and College regulations.
- Enrolment onto a specific session of the appropriate programme on the LMS.
- Registration with partner college where applicable – this additional step will be subject to the partners QA process.

4. ORIENTATION AND INDUCTION

International learners and learners requiring additional supports may require an additional orientation. This will be agreed when the applicant registers.

All learners are invited to an induction process organised by the school to introduce them to the college community, student supports, amenities etc.

5. GLOSSARY

Applicant – an individual who has applied for a place on any programme offered by IBAT and who has not yet registered.

Learner – an individual who has been accepted onto a programme and fulfilled the obligations required to be registered with the college and has completed the registration process.

Student – the term used for learner in learner-facing documents such as the Student Handbook, Student Card or Code of Conduct.

Registration – A process where the credentials of an applicant (in receipt of an unconditional offer) are authenticated and the required information is collected and recorded on the Learner Management System.

Enrolment – a process where a learner, registered with the College, is formally linked to a particular programme or module to which they have been formally admitted.

Programme – a defined course of learning leading to an award accredited externally or not.

Module – a subset of a programme.

SOP 2.4 The 5 Stage Model of e-moderating – Teaching online and supporting online learners

Guided and adapted to align with the College academic framework (QAH 6.2) of IBAT College we are utilising Professor Gilly Salmon's five stage model of e-moderating (https://www.gillysalmon.com/five-stage-model.html#). It acts as a resource outlining the multifaceted role of the online lecturer where they are required to scaffold, facilitate, and moderate online learning while simultaneously providing various types of support to online learners.

We present below the following five stages of blended/online delivery.

- Module Access/Induction – (Weeks 1 & 2)

  Lecturer welcomes the learner and has materials ready on the VLE. IT support the learner in accessing the materials. The Programme Team and Registry are available to address frequently asked questions.

- Online Socialisation – (Weeks 1-4)

  Lecturer engages in ice-breaker type activities with the goal of creating a community of learners. Provide regular feedback and let learner know what they should be doing each week. All continue to answer questions and provide regular virtual 'office hours' ensuring that learners are able to interact with you in real time (synchronously) if they require direct support.

- Information Exchange (All weeks)

  The Student Affairs Coordinator monitors and supports learner engagement by reviewing attendance data and discussing engagement with lecturers.

  The lecturer ensures a range of learning materials and resources are available, accessible and clearly signposted throughout the duration of the module. They also provide authentic, real-world examples linked to materials and to retain engagement make links explicit between learning activities and assessment.

- Knowledge Construction; Facilitating Learning (All weeks)

  The lecturer facilitates individual, group and peer activities, guides discovery, provides different forms of feedback and creates communities of learning. The learner requires visibility of lecturers and the college addressing their questions and ongoing monitoring of engagement.

- Synthesise and Assessment (Week 4 – 15)

  The school needs to operate its virtual hours, Q&A, monitoring activities but in addition remind/reiterate to student's assessment requirements/timelines. Lecturers must incorporate time to review and synthesis of the module activities, and signpost where, when and how feedback will be presented.

SOP 2.5 Moodle Page Set-Up Checklist

To ensure a uniform format for all modules on any programme irrespective of delivery mode the Moodle Coordinator must ensure that the following information is displayed. To assist them in this activity a checklist is applied in the set-up of each module for each semester it is delivered.

VLE interface will be structured to provide access to resources based on simple login and the minimum of navigation.

All digital materials used in the teaching and learning on the programme will, where possible, be made available to the students within the VLE

Module / Diploma Title	
Semester / Intake	
Item	**Tick to ensure completed**
Welcome message from lecturer	
Lecturer Contact Details – name, email etc.	
Moodle page name	
Information about the module / professional diploma – learning outcomes, assessment strategy,	
Google Class Meets link generated	
Links to Meet recordings	
Labelled blocks of content	
Assessment details	
Assignment upload slot using plagiarism software, e.g. Turn-it-In or Vericite as appropriate	
Assignment Cover Sheet: Must have the following statement: "By checking the box below: I certify that this work is my own and is free from plagiarism. I understand that this work will be checked for plagiarism by electronic or other means and may be transferred and stored in a database for the purposes of data-matching to help detect plagiarism. The work has not previously been submitted for assessment in any other module or to any other institution.".	
Assignment due dates	
Academic Integrity video	

3 Operating Protocols and Procedures

OPP 3.1 Protocol on Dealing with Queries from the Press and Press Releases

Version	1	Status / Date
Owned by	Registrar's Office	
Approved by	Board of Governors	Approved Sept 2018
Reviewed	Board of Governors	September 2020

The most important consideration when dealing with the press is the reputation of the college, GUS and the accuracy of any press reporting.

An approach may be made by the press, for information, to any department. It is important that all staff are appraised of these protocols.

Protocol:

All approaches by the press must be directed to the Marketing Manager. In the absence of the Marketing Manager the College Principal, Head of School or Registrar must be informed. No staff member is authorised to represent the College to the press without clearance from the College Director. Personal communication with the press, in own time, must not reference the college or GUS.

Where the approach is routine and merely a request for information this can be managed by a member of the SMG. All data must be verified by the relevant department and checked by another member of the SMG. All correspondence must be in writing and copied internally for recording purposes.

Where the approach could be deemed hostile, a reputational risk or where it might be leading to further enquiries then all communication is channelled to the Marketing Manager who will notify the SMG: AND GUS Head of PR & Communications – see below for details.

Where there is a reputational risk to awarding bodies, accreditor or quality assurance agencies – QQI,ACELS, UWTSD the appropriate contact must be informed in advance of an publication, if known.

All press releases are to be prepared by the Head of Marketing and approved by the College Director and one other member of the SMG. Where the situation is reactive and negative any material supplied is also subject to the approval of the Head of PR & Communications – GUS – see below for details.

In all contact with the press is subject to the College policy on GDPR.

Rob Forbes - Head of PR & Communications
Global University Systems
30 Holborn, London, EC1N 2LX, United Kingdom
Direct: +44 (0)20 3005 6125
Switchboard: +44 (0)20 3435 4455
Email: Rob.Forbes@gus.global

OPP 3.2 Protocol on the College Being Notified of the Death of a Student

Version	1	Status / Date
Owned by	Registrar's Office	
Approved by	Board of Governors	Approved Sept 2018
Reviewed	Board of Governors	September 2020

The most important considerations when dealing with the death of a student are the dignity of the student and wishes of the family.

Protocol:

On notification of the death of a student the College Director and Senior Management Team are to be notified immediately. The College Director will appoint one of the three members of the SMG to manage the process – the nominated manager.

In cases of a sudden death or where the family have not been notified the nominated manager will contact An Garda Siochána who will contact next of kin.

When the Gardai confirm that the family have been properly notified the nominated manager will act as a point of contact for the family.

The nominated manager will then:

1. Contact the family to provide a point of contact and support and to determine the family wishes regarding communications (as appropriate) – this will be managed sensitively and unobtrusively.
2. In case of international students this may involve:
    a. Supporting the family to travel to Ireland and advise on accommodation etc.
    b. Assist with repatriation
    c. Assist with local arrangements if family cannot be present
    d. Arrange for personal possessions to be returned or disposed of.
3. Ensure the wider management team are aware of the situation and who the nominated manager is.
4. Ensure Reception (and switchboard) are aware that all queries are to be handled by the Marketing Manager.
5. Contact Marketing Manager to manage queries or implement press protocol (OPP2.1) as required.
6. Contact finance and library to ensure no fines, bills or invoices are sent to the students address
7. Contact Student Affairs to arrange counselling for classmates if appropriate
8. Contact HoS to ensure teachers are properly informed
9. Ensure Pearlway is updated to ensure no communication is made to the students address
10. Ensure relevant accreditors are informed and no correspondence is issued to student.

Follow up:

- Book of Condolences as appropriate
- Liaise with learners regarding details of funeral service

The College Director and SMG should also consider:

- Holding memorial service if appropriate

- Handling posthumous awards or noting the achievement of the student at the appropriate graduation event.

Where there are financial implications, arrangements are subject to the approval of the College Director.

OPP 3.3 Protocol on the College expelling a Student

Version	1	Status / Date
Owned by	Registrar's Office	
Approved by	Academic Council	Approved 30.04.21

A student may be withdrawn from a programme for disciplinary reasons such as Severe Academic Misconduct (QAH, section 8.16.4) or for disciplinary reasons an expulsion is required, under the penalties determined by the Student Disciplinary Committee (QAH, section 7.16.5).

The Office of the Registrar is required to record, inform and handle all matters relating to the expulsion. This entails:

11. Prior to issuing notification liaise with finance, Student Recruitment & Library if any outstanding fees, fines or materials have to be returned.
12. Issue a formal notification to the student concerned outlining the reason for the expulsion, the forum where the decision was made, the appeals process, the timeframe and any applicable charge.
13. Record this decision in the student's profile in Pearlway or CLASS.
14. Ensure relevant accreditors are informed and no correspondence is issued to student.
15. In case of international students this will involve:
    (a) Notifying INIS of the exiting of the student from their programme of study.
16. Notify Academic Council of the expulsion decision.
    (a) Only the student number and the forum where the decision was made will be disclosed to respect the privacy of the student concerned.
17. Contact HoS to ensure teachers are properly informed and that the student is not in attendance going forward.
18. Contact Reception to inform aa member of the Registry Team is an expelled student is on campus.

Where there are financial or legal implications, arrangements are subject to the approval of the College Director / Interim Managing Directors.

OPP 3.4 Protocol on addressing the Planning questions and key considerations in Stage 1 (Analysis) of ADDIE (ISD)

Context	Planning Questions	Considerations
Module/ Programme/ School Influences	1. Who are the teaching team that will contribute to the development of this module. What are the respective roles of contributors? 2. What is the broader context for your module in terms of the programme, school, faculty, professional bodies, or the community? 3. Are there industry or professional standards which impact on what you include in your module? 4. What time commitments are involved in the development and/or teaching?	• Identify how your module fits in the broader programme, check other modules to achieve balance and cohesion with such things as assessments due dates and use of educational technologies. • Consider what online teaching experience and level of digital knowledge or skills your teaching team have.
Teaching/ Learning Environment	1. What is your current teaching environment? 2. Is there the infrastructure or resources to support the use of educational technologies?	• Identify where the learning will take place: on-campus, across multiple campuses, industry and community locations or online.
Teaching/ Learning Approach	1. What is the current culture regarding teaching and learning in your school or unit. Will blended/online learning fit with this culture? 2. How will a blended/online learning approach improve the student learning outcomes?	• Consider if planned online assessments and learning activities will still be viable if student numbers increase or decrease.

Context	Planning Questions	Considerations
	3. Will the blended/online learning elements be scalable?	
Student Cohort	1. Who will be the typical student that will take this module or programme? 2. What is the context of their learning e.g. their level (first year or later years), their previous experience. What do students already know and what they should know after completing the module. 3. What is your cohort size? The number of students you have can constrain or provide opportunities for incorporating collaborative learning activities and group tasks.	• Do they have particular needs that you should consider. • Consider their experience of blended/online learning, their digital and online learning skills • For example, group discussions with twenty versus sixty may need a tutor or teaching assistant to moderate, or break the larger groups into smaller discussion groups.

OPP 3.5 Class Outing Disclaimer

Teacher:	
Group Name:	
Destination:	
Date & time of outing:	
Are their cost implications –	
College	
Student	
College & Student	

APPROVAL GRANTED BY HEAD OF SCHOOL Yes ❒ No ❒

HoS Signature _____

Note to the teacher: Please make sure all students participating on the outing sign below.

To the student(s): Please sign below if you wish to go out on the trip to (the) _____

Please ensure that you always stay with the group and teacher; if you fail to do so, neither IBAT College, nor the teacher will be responsible for anything that happens to you during the class outing.

	First Name	Last Name	Departure Time	Return Time	Signature
1					
2					
3					
4					
5					
6					
7					
8					
9					

10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					

OPP 3.6 Consent Form – Recording / Filming / Photography

Please read carefully and provide consent if agreeable

I hereby consent to IBAT College Dublin using images of myself captured in audio/video recordings, and/or photographs, taken/recorded by IBAT College Dublin.

I consent to them being used for marketing and publicity related purposes and to their use in other IBAT College Dublin publications. I understand that they may be published on social media channels or on the IBAT College Dublin website, other websites or elsewhere.

I understand that:

- My images will be held in accordance with the GDPR guidelines (the General Data Protection Regulation):
- The images of myself captured in the video recordings and/or photographs will be the copyright of IBAT College Dublin and any other intellectual property which arises in the photographs/recordings will also belong to IBAT College Dublin;
- I hereby agree to irrevocably assign all property rights in my photographs and/or recordings to IBAT College Dublin;
- I hereby agree to waive all rights in my performance in the film and/or recordings to IBAT College Dublin.
- I can ask IBAT College Dublin to stop using my images at any time, in which case efforts will be taken to prevent them being used in future digital and offline publications but they may continue to appear in publications already in circulation.

If the recording is going to capture me speaking (e.g. an interview, presenting information, etc), I also agree that I will only include any material in the recording which is the intellectual property (including copyright) of another party, if I have their permission or a licence to do so and irrevocably licence IBAT College Dublin to use and sub-licence any copyright in the words spoken (once fixed by the recording).

Full Name:

Email Address:

Date of Consent:

Signature: