etbi
Education and Training Boards Ireland
Boird Oideachais agus Oiliúna Éireann

DATA PROTECTION

POLICY

For all staff in Education and Training Boards Ireland

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Data Protection Policy

This policy must be brought to the attention of all staff/seconded contractors/consultants/agents to include any entity or individual action for or on behalf of employed directly by ETBI, through an agency to ETBI and seconded to ETBI, including those on approved leave of absence.

ETBI will provide this code to all staff through appropriate means (e.g., direct correspondence, SharePoint, CPD, induction and mentoring programmes and/or on ETBI website).

Any queries in relation to ETBI Data Protection Policy & Procedure should be communicated to the HR/IR Governance Officer in the first instance.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

CONTENTS

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

1. POLICY

1.1 Overview

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data. The Education and Training Boards Ireland (ETBI) needs to collect and use personal data about its staff and other individuals who come into contact with the organisation. This Data Protection Policy provides information about the ways in which ETBI collects, stores and uses personal data relating to individuals (data subjects) or personal data received by ETBI indirectly (via a third party). ETBI is the Data Controller of personal data and is subject to the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation (GDPR) 2016/679.

ETBI is not required to appoint a designated Data Protection Officer (DPO), under the GDPR requirements.

This policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

ETBI is committed to complying with all applicable Data Protection, privacy and security laws and regulations.

The Data Protection policies adopted by ETBI create common cores set of values, principles and procedures intended to achieve a standard set of universal compliance parameters based on GDPR.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

1.2 Purpose

ETBI intends to meet all relevant Data Protection, privacy, and security requirements, whether originating from legal, regulatory, or contractual obligations.

ETBI as a Data Controller, has established this Policy as an EU Data Protection Framework to comply with all relevant European Data Protection requirements and has aligned same to relevant internal policies, programs, and controls. In particular this document sets out ETBI's policy regarding Personal Data collection/processing/sharing in ETBI.

ETBI also embraces Privacy by Design and Privacy by Default principles in all its services and functions both current and future. This ensures that the public can maintain a high level of trust in ETBI 's competence and confidentiality while handling data.

This policy should not be viewed in isolation. Rather, it should be considered as part of ETBI's suite of Data Protection policies and procedures (see Appendix A for a list of Compliance Policies).

1.3 Scope

All Data Protection Policies apply to:

- Any person who is employed by ETBI who receives, handles or processes personal data in the course of their employment.
- Third party companies/individuals (data processors) that receive, handle, or process personal data on behalf of ETBI .

This applies whether you are working in ETBI's headquarters, travelling or working remotely.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

1.4 Policy Compliance

Compliance

Compliance with our data protection policies will help protect ETBI against data breaches under data protection legislation, reputational damage to ETBI and/or an infringement of the rights of employees, or other relevant third parties.

Compliance Exceptions

Any exception to the policy shall be reported to the Director of Organisation Support and Development (Internal) in advance.

Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with ETBI's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

2. ROLES AND RESPONSIBILITIES

ETBI Board	To review and approve the policy on a periodic basis.
The General Secretary & the Executive Leadership Team	The General Secretary and the Executive Leadership Team (ELT) is responsible for the internal controls of ETBI, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. Responsible for: • Reviewing and approving all Data Protection Policies and any updates to them as recommended by the HR/IR Governance officer or Legal Services Support Unit (LSSU). • Ensuring ongoing compliance with GDPR in their respective area of responsibility. • As part of ETBI's Annual Statement of Internal Control, signing a statement which provides

	assurance that their functional area is in compliance with GDPR. • Ensuring oversight of data protection issues in their functional area. • To lead the Data Protection compliance for their Section/Function. • Provide guidance to their staff. • Ensure prompt reporting of data protection breaches originating from their Section/Functional area.
	• The GS/ELT may on advisement delegate this function to a specialist - either person or LSSU.
Director of Organisation Support and Development (Internal) and HR/IR Governance Officer.	• To lead the Data Protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including GDPR. • To advise on all aspects of Data Protection and Privacy obligations. • To monitor and review all aspects of compliance with Data Protection and Privacy obligations. • To act as a representative of Data Subjects in relation to the processing of their personal data. • To report directly on Data Protection risk and compliance to the General Secretary, Financial Audit Risk (FAR) Committee and ETBI's Governing Body.
Staff/External Parties	• To adhere to the suite of Data Protection Policies. • To report suspected breaches of policy to their line manager/Directorate.
General Secretary	• The General Secretary has overall responsibility for the delivery of the regulatory objectives of ETBI including compliance with Data Protection and privacy obligations.

3. PRINCIPLES OF DATA PROTECTION

3.1 Personal Data Processing Principles

The following Data Protection requirements apply to all instances where Personal Data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

ETBI has established the following high-level principles relating to Data Protection in order to comply with relevant European requirements.

- Personal Data shall only be processed fairly, lawfully and in a transparent manner (**Principles of Lawfulness, Fairness and Transparency)**
- Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes **(Principle of Purpose Limitation**)
- Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**Principle of Data Minimisation**)
- Personal Data shall be accurate, and where necessary kept up to date (**Principle of Accuracy**)
- Personal Data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes of which the Personal Data are processed (**Principle of Data Storage Limitation**)
- Personal Data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:

    i. prevent and / or identify unauthorised or unlawful access to, or processing of, Personal Data; and
    ii. prevent accidental loss or destruction of, or damage to, Personal Data (**Principles of Integrity and Confidentiality**)

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

ETBI whether serving as a Data Controller or a Data Processor, shall be responsible for, and be able to demonstrate compliance with, these key principles (**Principle of Accountability**).

3.2 Lawful Processing and Consent

ETBI as a Data Controller, shall be responsible for, and be able to demonstrate compliance with these GDPR requirements.

- to process Personal Data in accordance with the rights of Data Subjects and to communicate with Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear language.

- only transfer Personal Data to another group or Third Parties outside of the European Economic Area (EEA) in accordance with this Policy.

- conduct all Personal Data processing in accordance with legitimate GDPR based processing conditions in particular:

- Data Subject Consent for one or more specific purposes, and / or
- Necessary processing for contract performance or contract entry.

  and / or
- Legislative/statutory basis underpinning Processing.

Consent

For processing based on consent, each functional area must demonstrate that the data subject has provided appropriate consent for the specific processing. Further consent must be obtained for any new processing activity outside of initial consent, including data aggregation activity either for use by ETBI or by third parties on behalf of ETBI.

In particular, Data Processing Consent cannot be implied and must be:

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

- Freely given,
- Specific,
- Informed,
- Unambiguous and
- Provided by an affirmative action (Opt-in as opposed to Opt-out)

Appropriate Consent Request methods include:

- Check boxes on replies to applications or forms, and / or
- Click boxes on online forms where Personal Data is entered, and / or
- Clauses in contracts with vendors.

Any written Consent Request must be:

- Clearly distinguishable from other matters and
- Presented in clear and plain language

Each functional area shall establish collection and documentation processes for Data Subject Consent to the Processing, and / or transfer of Personal Data. These processes shall include:

- Provisions for determining what information must be provided in order to obtain a valid Consent,
- Recording the communication of that information to the documentation of the date of Consent including validity, scope and equity of the Consents given.

Each functional area shall establish Consent Withdrawal processes and inform Data Subjects about:

- their right to withdraw consent at any time and the process through which they can achieve this.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Processing of Special Categories of Personal Data

ETBI will not process Special Categories of Personal Data unless:

- The Data Subject expressly consents and / or
- It is necessary to carry out Data Controller's obligations or exercise Data Subject's specific rights in the field of employment and social security and social protection law

and / or

- It is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.

It is in the vital interest of the data subject ETBI may only process such data where it is necessary to protect a data subject's vital interest in the event that this subject is physically or legally incapable of giving consent. For example, this may apply where the data subject may require emergency medical care. Only ETBI may authorise this exemption and only in accordance with relevant national legislation.

Any exceptions to processing in the absence of one of these conditions requires the approval of General Secretary or the Director of OSD (Internal).

3.3 Transparency – Data Protection Notices (Fair Disclosure Notices)

To ensure fair and transparent processing activities, must provide Data Protection Notices to Data Subjects when directly collecting data. This Policy includes Data Protection Notices for Staff and for Recruitment Candidates.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

These notices must be:

- Provided at the first contact point with the Data Subject or as soon as reasonably practicable.
- Provided in an easily accessible form.
- Written in clear language.
- Made in such a manner as to draw attention to them.

If ETBI use Consent as the Processing Personal Data condition, then this Consent should, where possible, be obtained at the data collection point.

Each Functional area collecting Personal Data must establish technical or administrative means to:

- Deliver the Date Protection notices and
- Document that ETBI has provided these notices to the Data Subject at the time of collection, or document they were previously provided and
    - Record all obtained Consents and ensure this information is up to date.

See Appendix B, and C for Data Protection Notices for Recruitment Candidates and Staff.

If the functional area intends to process Personal Data for an additional process outside of original consent, then they must get the Data Subject's additional consent through an additional Data Protection notice or other suitable notification.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Wherever possible, these Data Protection notices should be given at the first point of contact with the Data Subject or, if it is not possible on collection, as soon as reasonably practicable thereafter, unless otherwise agreed with the Director of OSD (Internal).

In the case of employees, the Data Protection notice should be referred to in the employment contract. Appropriate Data Protection notices should also be referred to in any job application form, or other internal employment document. The disclosures should be made in a manner calculated to draw attention to them.

3.4 Data Collection from Third Party Sources

In addition to Section 3.3 above, when ETBI collects Personal Data from a Third Party (i.e. not directly from a Data Subject), the Data Controller must provide Data Protection notices to the Data Subject either at the time of collection or within a reasonable timeframe that is no more than 30 days post collection.

In addition to the content of the notice outlined above in Section 3.3, Functional area shall provide the Data Subject with the following information necessary to ensure fair and transparent processing of their Personal Data:

- The Personal Data collected
- Whether this was from a public source.
- The categories of Personal Data concerned.

The following are the only exceptions:

- If the Data Subject has already received this information or
- Notification would require disproportionate effort or
- The law expressly provides for this Personal Data collection, processing or transfer.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

3.5 Data Minimisation and Retention

Each functional area should limit Personal Data collection to:

- What is directly relevant and
  - What is necessary to accomplish a specified purpose.

Each functional area should identify the minimum amount of Personal Data needed for a particular purpose and then align collection volumes and associated retention periods to this purpose.

Please see ETBI 's Data Retention Policy and Schedule.

3.6 Data Use Limitation

ETBI must only collect Personal Data for specified explicit and legitimate purposes. They are prohibited from further processing unless they have identified and documented additional legitimate processing conditions or if the Personal Data involved is appropriately Anonymised and /or Pseudonymised and used for statistical purposes only. Please see Section 3.12 below for further information.

3.7 Data Accuracy

ETBI must ensure that any Personal Data collected is complete and accurate and maintained in an accurate, complete and up-to-date form as its purpose requires.

3.8 Data Storage Limitation

ETBI must only keep Personal Data for the period necessary for permitted uses. They shall establish a destruction date and / or review schedule when defining a Personal Data permitted use under the stated purpose. This shall be recorded and aligned to ETBI 's Data Retention Policy and Schedule.

ETBI should reasonably endeavor to erase any Personal Data that violates:

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy

- If ETBI no longer requires the Data
- If the Personal Data, no longer benefits the Data Subject in the relevant process

ETBI should Anonymise and / or Pseudonymise Personal Data where possible rather than erase if:

- The law prohibits erasure
- Erasure would impair the legitimate interests of the Data Subject
- Erasure is not possible without disproportionate effort due to the specific type of storage or
- Where the Data Subject has disputed the accuracy of the Personal Data, ETBI disagrees with that assertion and resolution has not been reached.

3.9 Security of Personal Data (Integrity and Confidentiality)

Information Security

ETBI shall ensure Personal Data security through appropriate physical, technical and organisational measures. These security measures should be in keeping with standards appropriate to ETBI and prevent:

- Alteration
- Loss
- Damage
- Unauthorised processing
- Unauthorised access

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

When implementing Personal Data security measures each functional area must consider:

- Technological developments
- Implementation Costs
- Nature of relevant Personal Data
- Inherent Risks posed by human action/physical/natural environment

IT, Communications & Facilities Officer will adequately address European Data Protection requirements to relevant ETBI IT Policies and Procedures.

European Data Protection requirements specifically refer to Personal Data collected and processed within Europe. However, ETBI is committed to protecting all collected, processed, stored and transferred Personal Data regardless of country of origin.

3.10 Data Breach (Unauthorised Disclosure)

No employee or agent shall disclose Data Subject's Personal Data (including Personal Data or Special Categories of Personal Data), except where this Policy allows such disclosures.

Staff must report all suspected incidents of unauthorised access to their line manager. Incidents include disclosure, loss, destruction or alteration of personal data, regardless of whether it is in paper or electronic form. Functional area must establish formal procedures and a point of contact to report all potential unauthorised disclosure incidents.

Please see ETBI 's Data Breach Management Guidelines in Appendix D

3.11 Data Encryption

ETBI has drafted guidelines for staff on the encryption of Personal Data contained, processed or transmitted within hardware and software resources that are owned and/or operated by ETBI.

Situations Requiring Encryption – Data at Rest (Servers, Desktop Computers, Laptops, Tablets, Mobile Phones and other Smart Devices and Removable Storage Devices) and Data Transmission.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

3.12 Data Anonymisation/Pseudonymisation

Anonymisation and Pseudonymisation are two methods of processing personal data, in such a manner that the Personal Data in question cannot be traced back to the individual (Data Subject) to whom it originally pertained. The key difference between these methods as defined under GDPR, is whether the original data subject can be re-identified.

Anonymisation renders the data subject unidentifiable, even to the party that carries out the anonymisation of data. If the data is truly anonymised and identifying the subject is impossible, then the data falls outside the remit of GDPR.

Pseudonymisation renders the data subject unidentifiable without the use of additional information. Once the "additional information" and the pseudonymised data are held separately, the data processor/controller can use the data more freely, as the rights of the data subject under GDPR remain intact.

4. DATA PROTECTION PRACTICE / ACCOUNTABILITY REQUIREMENTS

Privacy by Design is an essential requirement that involves minimising privacy risks to individuals. It is the consideration of data protection implications at the start or re-design of any product, service, system, IT application or process that involves the processing or personal data. It fosters a culture of embedding privacy by design into operations and ensuring proactivity instead of reactivity.

Privacy by Default promotes that, where possible, having regard to business implications and the rights of the data subject, the strictest data protection settings are applied automatically to any project.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

ETBI has an obligation under GDPR to consider Data Privacy throughout all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to Personal Data. This is of particular importance when considering new processing activities or setting up new procedures or systems that involve Personal Data. GDPR imposes a 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought. Each functional area engaged in projects, new courses, services or systems development of any sort (including change to existing practices) through the relevant local project and change management processes must comply with the terms of this Policy.

4.2 Data Protection Impact Assessment (DPIA)

When ETBI undertakes a processing activity which would be likely to have a privacy impact upon staff, they should consider if a Data Protection Impact Assessment is required. A Data Protection Impact Assessment (DPIA) is a tool, required by GDPR, which can help ETBI to identify the most effective way to comply with its Data Protection obligations as well as meeting individuals' expectation of privacy by facilitating the identification and remediation of risks in the early stages of a project. It should also identify measures which would help to reduce risks. Therefore, DPIA's are an integral part of taking a Privacy by Design approach to processing of Personal Data.

When the Processing of Personal Data may result in a high risk to the rights and freedoms of a Data Subject, Functional area are required to conduct a DPIA and then consult with the Director of OSD. Where the requirement for a DPIA has not been established, or where there is any confusion as to the applicability of Data Protection requirements, a referral must be made to the DPO and the Privacy by Design principles.

Such assessment is also recommended for high-risk data processing, which was in place before May 2018 to ensure that the Privacy risks to individuals are still mitigated.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

ETBI's Data Protection Impact Assessment (DPIA) Form can be found in Appendix E and DPIA Criteria and Guidelines in Appendix F.

4.3 Record of Processing Activity and Data Inventories

ETBI as a Data Controller is required under GDPR to maintain a record of processing activities (ROPA) under its responsibility. That record contains details of why the Personal Data is being processed, the types of individuals about which information is held, who the Personal Data is shared with and when such Data is transferred to countries outside the EU.

New activities involving the use of Personal Data that is not covered by one of the existing records of processing activities require consultation with the Director of OSD prior to the commencement of the activity.

Each ELT in their own section will review records of processing periodically and will update same accordingly.

See Appendix G for ETBI 's ROPA

Maintenance of Data Processing Inventories

Functional area must maintain a written records of processing activity under its responsibility on a system accessible to the Director of OSD. These are known as Data Inventories or Data Processing Registers, a template of which is available in Appendix I. The Director of OSD will review these records periodically and will update same accordingly. The Director of OSD will provide Processing Activity records to a Supervisory Authority (Office of the Data Protection Commissioner) on request.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

4.4 Transfer and Sharing of Data

Sharing with a Third Party or External Processor

As a general rule, Personal Data should not be shared with or passed on to third parties, particularly if it involves Special Categories of Personal Data but there are certain circumstances when it is permissible e.g.

- The Data Subject consents to the sharing.
- The third party is operating as a Data Processor and meets the requirements of GDPR. Where a third party is engaged for processing activities there must be a written contract or equivalent in place which shall clearly set out respective parties responsibilities and must ensure compliance with relevant European and local Member State Data Protection requirements/legislation. These are known as Data Sharing Agreements.

The Director of OSD should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

Transfer of Personal Data outside the EEA

Transfers of Personal Data to third countries are prohibited without certain safeguards. The means ETBI must not transfer Personal Data to a third country unless there are adequate safeguards in place which will protect the rights and freedoms of the Data Subject. It is important to note that this covers Personal Data stored in the cloud as infrastructure may be in part located outside of the EU/EEA.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Functional area must not transfer Personal Data to a third party outside of the EU/EEA regardless of whether ETBI is acting as a Data Controller or Data Processor unless certain conditions are met.

Prior to any Personal Data transfer outside the EU/EEA, the General Secretary, (on the recommendation of the Director of OSD) must approve the transfer of such information and record the determination in writing.

4.5 Third Parties Relationships and Data Sharing Agreements

Where ETBI engage a third party for processing activities, the Data Processor must protect Personal Data through sufficient technical and organisational security measures and take all reasonable compliance steps. When engaging a third party for Personal Data processing, ETBI must enter into a written contract, or equivalent. This contract known as a Data Sharing Agreement and must:

- clearly set out respective parties responsibilities
- ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

and must give due consideration to the following items:

- Management of Data Processors
- Selection of Data Processors
- Contract Requirements
- Sub-contracted Data Processors
- Monitoring and Reporting

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

- Data Transfers
- Appropriate Safeguards
- Derogations for specific situations
- Once off transfer of Personal Data
- Data Sharing Agreements
- Review of data sharing arrangements
- Data transfer methods
- Email
- Cloud storage and cloud applications
- Telephone / mobile phone
- Sending the information by post
- Hand delivery / collection
- Data Breach Notification

5. DATA SUBJECT RIGHTS

The ELT shall maintain appropriate processes and procedures to address Data Subjects rights under GDPR.

Data Subjects have the following rights under Data Protection Law, subject to certain exemptions, in relation to their personal data:

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Right	Explanation
Information	The right to be informed about the data processing ETBI does.
Access	The right to receive a copy of and/or access the personal data that ETBI holds about you.
Portability	The right to request that ETBI provides some elements of your personal data in a commonly used machine readable format in order to provide it to other organisations.
Erasure	The right to erasure of personal data where there is no legitimate reason for ETBI to continue to process your personal data.
Rectification	The right to request that any inaccurate or incomplete data that is held about you is corrected.
Object to processing	The right to object to the processing of your personal data by ETBI in certain circumstances, including direct marketing material.
Restriction of processing concerning the data subject	The right to request the restriction of processing of personal data in specific situations where: (i) You contest the accuracy of the personal data; (ii) You oppose the erasure of the personal data and request restriction instead; (iii) Where ETBI no longer needs the data but are required by you for the establishment, exercise or defence of legal claims.
Withdraw Consent	If you have provided consent for the processing of any of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. This can be done by contacting the person who obtained that consent or ETBI 's (contact details below).
The right to complain to the Data Protection Commissioner	You have the right to make a complaint in respect of our compliance with Data Protection Law to the Office of the Data Protection Commissioner.

In order to exercise any of the above rights, please contact a representative of the Director of OSD using the contact details in Section 9 below.

5.1 Subject Access Requests (SARs) and Subject Rights Requests (SRRs)

Employees of ETBI can contact their line manager to discuss their request requirements prior to making a formal request in order to maximise the likelihood that their request will be fulfilled in a timely, efficient, and satisfactory manner. External requests for personal data should all be directed to the Director of OSD for response.

All Subject Access Requests are requested to be made via the Request Forms that are available on ETBI website. All subject access requests shall be directed to the Director of OSD, and all requests shall have an open status until an action by the Director of OSD sets a closed status.

Any information provided to a Data subject in response to a request must be:

- Concise
- Transparent
- Intelligible
- In an easily accessible form, using clear and plain language
- Free unless proven to be excessive (administration fee chargeable in this case) and
- Provided in a timely manner.

Each Functional area must notify the Director of OSD immediately when in receipt of a Data Subject Request and must provide the Director of OSD with all necessary support to allow a response in accordance with regulatory timelines.

See Appendix H and I for ETBI 's Subject Access Request Form and Subject Rights Request Form.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

5.2 Fees and refusals of SARs under GDPR

There is no fee for Subject Access Requests. However, under GDPR, ETBI reserves the right where requests from a data subject are manifestly unfounded or excessive in nature to either:

- Charge a fee to cover the administrative costs of providing the personal data or
- Refuse to act upon the request.

ETBI may also refuse to act upon a subject access request under GDPR in the following circumstances:

- Where it would breach the rights of someone else.
- Where it is the subject of an ongoing legal case.
- It would be illegal to do so.
- The identity of the requester cannot be determined.
- Where existing processes exist to access personal data (a charge may be in place).

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

6. PERSONAL DATA PROTECTION INCIDENT RESPONSE AND BREACH NOTIFICATION

6.1 Data Breach

ETBI as a Data Controller is legally required to notify the Office of the Data Protection Commissioner where a personal data breach is likely to result in a risk to data subjects' rights and freedoms.
In addition, ETBI are legally required to notify affected individuals (Data Subjects) where a Personal Data breach is likely to result in a high risk to their rights and freedoms. For further guidance on recognising and
managing a data breach, please see ETBI Data Breach Management Guidelines in Appendix

ETBI is required to notify the Data Protection Commissioner within 72 hours after having become aware of the Personal Data breach. Therefore, ETBI have to implement robust processes and procedures in place to identify and report suspected Personal Data breach incidents.

7. These procedures should also cover errors and "near misses" for learning opportunities and in order to mitigate possible future risks.

8. ETBI also have to implement an internal reporting procedure. This should include documentation of any suspected Personal Data breach, comprising the facts relating to the breach, its effects and the remedial action taken. Failure to report a notifiable breach could result in enforcement action by the Data Protection Commissioner including the imposition of an administrative fine in addition to any fines imposed regarding the breach.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

9. Please see Appendices J and K for ETBI's Procedures for reporting personal data and data breach notification form.

7. CCTV

All usage of CCTV other than in a purely domestic context must be undertaken in compliance with the requirements of the Data Protection Acts. Extensive guidance on this issue is available on the Data Protection Commissioner's website at:

Guidance on the use of CCTV | Data Protection Commissioner

In summary, all uses of CCTV must be proportionate and for a specific purpose. As CCTV infringes the privacy of the persons captured in the images, there must be a genuine reason for installing such a system and such purpose must be displayed in a prominent position.

ETBI 's CCTV Policy (in development).

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2025
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

8. TRAINING – EDUCATION AND AWARNESS

ETBI is committed to the provision of Data Protection training to ensure all individuals are aware of their respective obligations under Data Protection regulation. This is especially important for staff who handle Personal Data and / or Sensitive Category Personal Data in the course of their everyday business.

To achieve this, ETBI supports the development, rollout and communication of data protection training and an awareness programme across ETBI. This training programme ensures that staff are regularly reminded of policies throughout the year and refresher sessions, briefings and reminders occur at regular intervals. ETBI has also introduced an online GDPR training module for all staff. For online training and electronic communications, confirmation of reading and tracking of responses can be put in place to ensure staff follow through on a commitment to be aware of the policies. All sections, offices and staff are expected to:

- Acquaint themselves with, and abide by, the rules of the full suite of Data Protection Policies;
- Read and understand all Data Protection Policies;
- Understand what is meant by 'Personal Data' and 'Sensitive Category Personal Data' and know how to handle such data;
- Not jeopardise individuals' rights or risk a contravention of the Act;

ETBI must ensure that all staff are trained on relevant Privacy, Data Protection and Information Security requirements. This should be refreshed annually. In addition to General Data Protection Regulation training, staff may receive additional training when applicable to their duties or position. ETBI will maintain employee GDPR training completion records.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

9. MONITORING AND COMPLICANCE DEMONSTRATES ACCOUNTABILITY / INTERNAL CONTROLS

ETBI monitors compliance with Data Protection policies and procedures by maintaining of Data Inventory, compliance with Data Retention Schedule, staff training records, actions taken of recommendations following data breaches and near misses.

In order for ETBI to demonstrate compliance with the Data Protection Principles, ETBI have to put in place comprehensive governance measures. In addition, to the requirements set out above in Section 3.1 of this Policy, the GDPR requires:

- ETBI to maintain records of its processing activities, which must also be provided to the Director of OSD upon request.
- Further information regarding maintaining these records can be found in the Record of Processing Activity in Section 4.3 above.
- ETBI should ensure that they have implemented and documented procedures and procedures to comply with each of the minimum requirements outlined in this Policy.

10. SUPERVISORY AUTHORITY (DATA PROTECTION COMMISIONER)

Authority (Data Protection Commissioner)

The Office of the Data Protection Commissioner (DPC) is the Irish Statutory Authority for GDPR. Please see https://www.dataprotection.ie/ for further information on the Office of the Data Protection Commissioner.

11. CHANGES TO ETBI DATA PROTECTION POLICY

This Data Protection Policy will be subject to revision at least every 2 years. If you have any comments or queries in relation to this Data Protection Policy, please forward same to a representative of the Director of OSD at the contact details provided in Section 9 above.

12. APPENDIXES

Appendix A - ETBI's Suite of Compliance Policies

- Data Protection Policy
- Data Protection Notice for Staff
- Data Protection Notice for Recruitment Candidates
- Clean Desk Policy
- Data Retention Policy and Schedule • CCTV Policy (in development).
- Record of Processing Activity (ROPA)
- Acceptable Usage Policy (in development)

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Appendix B - Data Protection Notice for Recruitment Candidates

This privacy notice explains how the Education and Training Boards Ireland (ETBI) collects, stores, uses and shares your personal data. It also explains your rights in relation to the personal data we hold. ETBI is the Data Controller of your personal data and is subject to the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2016/679. For further information on ETBI's Data Protection Policies and Procedures.

For information on your rights as a Data Subject, please see the website of the Data Protection Commission *https://www.dataprotection.ie/*

As a candidate (job applicant) some of your personal data will be processed by ETBI. This data is collected from a variety of sources, mainly from yourself, but may also come from other sources e.g. your former employer(s), medical doctor.

ETBI may share information between different internal departments for operational reasons only as is necessary and proportionate for the purposes intended.

What information do we collect about you?

The types of personal data collected by ETBI include, inter alia:

- Name
- Date of birth (if provided)
- Nationality (if provided)
- Address
- Telephone number
- Email Address
- Details of previous employers
- Current Salary
- Schools/Colleges attended
- Qualifications
- Job application details and CV
- Citizenship and Work Permit number (if applicable)
- IP address and the type of device you are using when visiting ETBI website on a mobile device

Some of the information about you that ETBI holds is classified as special category data or sensitive personal data. In addition to the normal standards of confidentiality, we also

carefully control access to sensitive data within ETBI so that it is only available to those staff who require it to perform their duties.

Special Categories of personal data may be included in the following, such as:

- Health Declaration Form (from the Pre-Employment Medical Examination) and health data for purposes of disability support and/or public health
- Information on criminal convictions and pending court cases (as provided through Garda Vetting or Criminal Conviction Declaration Form)
- Racial or ethnic origins (as image in CCTV footage or in Visa and immigration details)

If provided on a **voluntary basis** by the candidate at recruitment stage, the following Special Categories of personal data may be processed by ETBI for the purposes of monitoring our performance against our strategic goal to be an equal opportunities employer:

- Gender Identity
- Disability
- Racial origin/ethnicity

How do we use the information about you?

The purposes for which ETBI may process your personal information include:

- ETBI processes your personal data for normal recruitment purposes. The information we hold to process is used to assess eligibility for the role applied for. We keep and use it to enable us to fulfil our obligations as an employer, and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process.
- Where Equality, Diversity and Inclusion information is voluntarily provided, ETBI will only ever share this information with third parties in a non-identifiable aggregated format for statistical insight.

Under data protection law, we are required to ensure that there is an appropriate legal basis for the processing of your personal data, and we are required to let you know what that basis is. The primary bases that we use are:

- processing that is necessary for the performance of our contract with you as an employer conducting a recruitment process
- processing that is required under applicable law ▪ processing that is necessary in the public interest and
- processing where we have your consent.

Does ETBI share your data with any third parties?

Below are some examples of when ETBI will release data about you to third parties (i.e. outside ETBI) where we have a legitimate reason in connection with your employment/potential employment/former employment to do so.

ETBI may share your relevant personal data with bodies including the following:

- Data Processors (sub-contractors used by ETBI in order to carry out a function on behalf of ETBI, e.g. cloud services provider Microsoft, Occupational Health Service, etc.)
- Former employers (to obtain References with your consent)
- Interview Board members
- Auditors
- Research funding bodies

This is not an exhaustive list and any other disclosures to third parties not listed here are made only where there is legitimate reason to do so and in accordance with the law.

Appendix C - Data Protection Notice for Staff

ETBI is the Data Controller of your personal data and is subject to the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2016/679. For further information on ETBI's Data Protection. For information on your rights as a Data Subject, please see the website of the Data

Protection Commission *https://www.dataprotection.ie/*

As a staff member, retiree or former staff member some of your personal data will be processed by ETBI. During the recruitment process, throughout your employment with us, and when your employment ceases, ETBI collects uses and stores (i.e. processes) your personal data. This data is collected from a variety of sources, mainly from yourself, but may also come from other sources e.g. your former employer(s) or your manager. During the course of your employment, additional information may be added to your record.

ETBI may share information between different internal departments for operational reasons only as is necessary and proportionate for the purposes intended.

What information do we collect about you?

The types of personal data collected by ETBI include:

- Name, date of birth, nationality and telephone numbers
- Addresses (current and past)
- Staff ID Number
- PPS Number
- Email Address
- Gender
- Next of kin/emergency contact details
- Marital/Civil Partnership status
- Details of previous employers
- Previous salary
- Previous pension details
- Educational History and Qualifications
- Job application details
- Citizenship
- Work Permit number
- Financial information, including bank details (BIC, IBAN, Name & Address of

- Bank/Building Society), PRSI class, tax details
- Training Records
- Access Control Records
- PMDS
- Leave records
- Disability information
- Health information, including medical certificates
- Details of criminal convictions (incl. as provided through Garda Vetting/Criminal Conviction Declaration Form)
- Image in CCTV footage/photography/filming
- Disciplinary/grievance records
- CV
- IP address and the type of device you are using when visiting ETBI website on a mobile device
- Car registration number (for travel expense claims)
- Call logs from work extension numbers

Some of the information about you that ETBI holds, such as health/medical details, is classified as Special Category Personal Data or sensitive personal data.

In addition to the normal standards of confidentiality, we also carefully control access to sensitive data within ETBI so that it is only available to those staff who require it to perform their duties.

How do we use the information about you?

ETBI processes your personal data for normal employment purposes. The information we hold and process is used for our management & administrative duties. We keep and use it to enable us to fulfil our obligations as an employer, and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, while you are employed by us and after your employment ends in line with our Data Retention Policy.

Under data protection law, we are required to ensure that there is an appropriate **Legal Basis** for the processing of your personal data, and we are required to let you know what that legal basis is. The primary bases that we use are:

- processing that is necessary for the performance of our contract with you

- processing that is required under applicable law
- processing that is necessary in the public interest and
- processing where we have your consent.

Where the processing of your personal data is based on your providing consent, you have the right to withdraw consent at any time by contacting the HR Department who obtained that consent, or Director of OSD (Internal).

The purposes for which ETBI may process your personal information include:

- Staff administration, including recruitment, appointment, training, promotion, progression, disciplinary matters, health, pension purposes and other employment related matters.
- Accounting & financial purposes, including pay, workforce planning & other strategic planning activities and to facilitate participation in schemes including Tax Incentive, etc. • Provision of wellbeing and support services
- To administer voluntary surveys of staff opinion about your experience of ETBI
- To include photos and video in print and electronic materials (e.g. prospectus, brochures, website, etc.) for promotional, press, documentation and archival purposes.
- Internal & external auditing purposes
- To meet health & safety obligations and equality of opportunity monitoring obligations
- To comply with statutory reporting requirements
- To produce reports and aggregated statistics for management and research purposes in order to plan and improve services
- To maintain a proportionate CCTV system for the specific purposes outlined in the CCTV Policy
- To assist with law enforcement where required or authorised by law
- To respond to requests for information made under Data Protection legislation or Freedom of Information legislation.

Does ETBI share your data with any third parties?

Below are some examples of when ETBI will release data about you to third parties (i.e. outside ETBI) where we have a legitimate reason in connection with your employment/potential employment/former employment to do so or with your consent.

ETBI may share your relevant personal data with bodies including the following:

- Data Processors (sub-contractors used by ETBI in order to carry out a function for ETBI, e.g. cloud services provider Microsoft, Occupational Health Service)

- Former employers for the purposes of obtaining references
- Department of Social Protection
- Revenue Commissioners
- Interview Board members
- Department of Public Expenditure & Reform
- Higher Education Authority (HEA)
- Comptroller & Auditor General
- Pension Authority
- Accounting firms for actuarial advice regarding pensions
- Internal and External Auditors
- Research funding bodies
- Central Statistics Office (CSO)
- Schemes including Tax Incentive, etc.

This is not an exhaustive list and any other disclosures to third parties not listed here are made only where there is legitimate reason to do so and in accordance with the law.

What are your rights under Data Protection Law?

You have the following rights, subject to certain exemptions, in relation to your personal data:

Right	Explanation
Information	The right to be informed about the data processing ETBI does.
Access	The right to receive a copy of and/or access the personal data that ETBI holds about you.
Portability	You have the right to request that ETBI provides some elements of your personal data in a commonly used machine readable format in order to provide it to other organisations.

Erasure	The right to erasure of personal data where there is no legitimate reason for ETBI to continue to process your personal data.
Rectification	The right to request that any inaccurate or incomplete data that is held about you is corrected.
Object to processing	You can object to the processing of your personal data by ETBI in certain circumstances, including direct marketing material.
Restriction of processing concerning the data subject	You can request the restriction of processing of personal data in specific situations where: (i) You contest the accuracy of the personal data (ii) You oppose the erasure of the personal data and request restriction instead (iii) Where ETBI no longer needs the data but are required by you for the establishment, exercise or defence of legal claims.
Withdraw Consent	If you have provided consent for the processing of any of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. This can be done by contacting the Department who obtained that consent or ETBI's Data Protection Office (contact details below).
The right to complain to the Data Protection Commissioner	You have the right to make a complaint in respect of our compliance with Data Protection Law to the Office of the Data Protection Commissioner.

In order to exercise any of the above rights please contact us using the contact details set out below.

Data Retention

ETBI will retain your personal data in accordance with our Data Retention Policy. The policy operates on the principle that we keep personal data for no longer than is necessary for the purpose for which we collected it. It is also kept in accordance with any legal requirements that are imposed on us. This means that the retention period for your personal data varies depending on the type of personal data.

Security – How we Protect your Personal Data

ETBI is committed to ensuring that your personal data is secure and with the Data Processors who act on our behalf. We are continuously taking technical and organisational steps to better protect your personal data. **Responsibilities of ETBI Employees**

As an employee of ETBI, you have a responsibility for any personal data relating to other people that you may access while employed by ETBI. This responsibility is in addition to any obligations arising from professional ethics or the Code of Conduct for Staff.

Staff must be fully aware of the importance of reviewing email correspondence before its issue. Staff should safeguard that the correct intended recipient and attachments have been selected prior to the issue of all email correspondence.

Staff who knowingly and recklessly disclose personal data to anyone who is not entitled to receive it or to seek to obtain data to which they are not entitled are in breach of Data Protection legislation and may be subject to ETBI's Disciplinary Procedures.

Website Privacy Policy

ETBI website privacy policy explains how data may be gathered about users of ETBI's website.

How ETBI will contact you

We may contact you by telephone, email or post. In order for us to have accurate information on record for you, it is important that you keep your contact details up to date. Please notify us if you change address or contact details.

Questions & Complaints

If you are unhappy with ETBI's handling of your personal data or believe that the requirements of data protection legislation may not be fully complied with, you should contact ETBI's

HR/IR Governance Officer in the first instance. You also have the right to submit a complaint to the Data Protection Commissioner.

How to contact us

Data Controller:

Please contact us if you have any questions about the information, we hold about you or to request a copy of that information.

ETBI –

- By email: james.eustace@etbi.ie
- In writing: Education and Training Boards Ireland, Piper's Hill, Naas, Co Kildare, W91K729
  • Tel: 045 901070

Office of the Data Protection Commissioner:

- www.dataprotection.ie
- By email: info@dataprotection.ie
- In writing: Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2, D02 RD28
- Tel: +353 57 868 4800 or +353 761 104 800

Appendix D - Data Breach Management Guidelines

Introduction

The Education and Training Boards Ireland (ETBI) is required under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a breach of security relating to personal data (hereinafter 'data breach'). The purpose of these Procedural Guidelines (the 'Guidelines') is to provide a framework for reporting and managing breaches involving personal data controlled and processed by ETBI. The Guidelines supplement ETBI Data Protection Policy which affirms ETBI's commitment to protect the privacy rights of individuals in accordance with data protection legislation, namely the EU General Data Protection Regulation ('GDPR') and Data Protection Act 2018. It is imperative for all

ETBI staff to immediately report any potential or suspected data breach to their line manager or Director of Organisation Support and Development by phone or email. If unsure whether an incident is a data breach or not, please refer to the guidance set out within this document.

Scope

The Guidelines apply to all processors of ETBI-controlled personal data, including:

- Any individual who is employed by ETBI or is engaged by ETBI who has access to ETBI controlled or processed personal data in the course of their employment or engagement for administrative, research and / or any other purpose;

- Individuals who are not directly employed by ETBI, but who are employed by contractors (or subcontractors) and who have access to ETBI controlled or processed personal data in the course of their duties for ETBI.

These Guidelines apply to:

- All personal data processed by ETBI in any format (including electronic and paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely;

- Personal data held on all ETBI's IT systems managed centrally by IT, Communications & Facilities Officer.

- Any other IT systems, including email and Cloud-based platforms on which ETBI controlled or processed personal data is processed.

What is a data breach?

Under GDPR, a data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error.

Data breaches may occur in a variety of contexts. For example:

- Loss or theft of data, including equipment on which data is stored (e.g. laptop, smartphone, tablet USB key etc.) or paper records

- Inappropriate access controls allowing unauthorised use of information (e.g., uploading personal data to an unsecured web domain, using unsecure passwords)

- Equipment failure

- Confidential information left unlocked in accessible area (e.g., leaving IT equipment unattended when logged into a user account)

- Disclosing confidential data to unauthorised individuals - Collection of personal data by unauthorised individuals

- Human error / accidental disclosure of data (e.g., emails containing personal or sensitive personal data sent to the wrong recipient)

- Hacking, viruses or other security attacks on IT equipment, systems, or networks

- Breaches of physical security (e.g., forcing of doors / windows / filing cabinets)

Whether an incident giving rise to the suspected data breach involves personal data must be determined on a case-by-case basis. If an incident does not involve personal data, it is not a data breach as per the GDPR definition. Furthermore, not all data incidents involving personal data will be data breaches.

For example:

- The personal data is securely encrypted or anonymised such to make the personal data unintelligible; and/or

- There is a full, up-to-date back-up of the personal data (in cases of accidental destruction).

Personal data is defined under GDPR as Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by ETBI.

Examples of personal data include, but are not limited to:

- Name, email, address, home phone number

- The contents of an employee HR file

- Notes of personal supervision, including matters of behaviour and discipline.

Processing is defined under GDPR as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Appendix E - Data Protection Impact Assessment (DPIA) Form

Data Protection Impact Assessment (DPIA) Form

You should start to fill out the template at the start of any **major project** involving the use of personal data, or if you are making a significant change to an **existing processing activity**. You should send the completed form to Director of Organisation Support & Development (OSD) (Internal) and the HR/IR Governance Officer. The final outcomes approved by the Director of OSD and integrated back into your project plan.

Details

Name	
Title	
Name of Controller (Directorate)	
Title of Controller (Line Manager/Project Lead)	
Name of new project or existing processing activity	
Date	

Step 1: Identify the need for a DPIA

Explain broadly (1) what the project aims to achieve and (2) what type of processing it involves.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and

using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the <u>context</u> of the processing: what is the nature of your relationship with the data subjects? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme?

Describe the <u>purposes</u> of the processing: what do you want to achieve? What is the intended effect on data subjects? What are the benefits of the processing (1) for you and (2) more broadly?
Is there a likely High Risk to the rights of Data Subjects? See Risk Example document attached

Step 3: Consultation process

Have you considered relevant stakeholders? Describe when and how you will seek stakeholders' views or justify why it's not appropriate to do so. Do you plan to consult information security experts or any other experts? Does your project involve any Data Processors Do you require a Data Sharing Agreement with your Data Processors?

Step 4: Assess Compliance with Data Protection Legislation

Describe compliance and proportionality measures. What is your Lawful Basis for processing? Does the project actually achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimisation In order to comply with the GDPR principle of Transparency, what information do you intend to provide to Data Subjects? How will you help to support Data Subject Rights What measures will you take to ensure Data Processors comply with GDPR Legislation? Does your project involve any international transfers of data and how do you intend to safeguard these transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact to Data Subjects Include associated compliance and corporate risks, as necessary.	**Likelihood of harm** Rare Unlikely Possible Likely Almost Certain	**Impact of harm** Insignificant Low Medium Major Severe	**Overall risk** Low Moderate High Very High Extreme

Step 6: Identify measures to reduce risk

Identify additional measures you could take to mitigate (reduce) or eliminate risks identified as Moderate to Extreme above in Step 5.					
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated Reduced Accepted	**Residual risk** Low Moderate High Very High Extreme	**Measure approved** Yes No	**Name, Position Date**
Residual Risks approved by Data Controller (line manager):					

Step 7: Review by Director of OSD and HR/IR Governance Officer

Summary of advice:	
Name & Date:	
This DPIA was noted at the meeting on	Date:

Step 8: Sign off by Director of OSD

Advice accepted? Y/N	Yes	No
If NO, you must explain your reasons:		
Data Controller Name	**Signed**	**Comments**
Notes This DPIA will kept under review by Director of OSD/HR/IR Governance Officer for the project and will review ongoing compliance with DPIA		

Appendix F - ETBI DPIA Criteria and Guidelines

Introduction and Explanation

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks at the start of any **major project** involving the use of personal data, or if you are making a significant change to an **existing processing activity**. The final outcomes should be integrated back into your project plan.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of data subjects, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether or not any remaining risks are justified. Therefore, a DPIA is a way to analyse the processing and identify and minimise data protection risks systematically and comprehensively. It is an important tool for building and demonstrating compliance with the GDPR principle of accountability.

When to use a DPIA?

The GDPR does not require a DPIA to be carried out for every processing operation. The carrying out of a DPIA is only mandatory where processing of personal data is *"**likely to result in a high risk to the rights and freedoms**" of data subjects (the person to which the data relates)* (Article 35 GDPR). When the functional area undertakes a processing activity which would be likely to have privacy impact upon employees, the public, patients, etc. they should conduct a DPIA of these risks and identify measures, which would help to reduce these risks. DPIAs are mandatory for any new high risk processing projects. It is also recommended for high-risk data processing which has taken place prior to May 2018 to ensure the privacy risks to individual are still mitigated. (For examples of risks please see Appendix A)

Even if there is no specific indication of likely high risk, it is good practice to conduct a DPIA at the start of any **major project** involving the use of personal data, or if you are making a significant change to an **existing processing activity** involving the use of personal data as a DPIA is a useful tool to comply with GDPR.

Please note that in some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a onetime exercise.

Identify the Need for a DPIA

In order to determine whether the processing is likely to result in a high risk the factors below should be considered. If you project involves any of the following you must carry out a DPIA.

Evaluation and scoring (including profiling and predicting), especially concerning a data subject's performance at work, economic situation, health, personal preferences, reliability or behaviour, location or movements. An example would be offering genetic tests in order to assess or predict disease/health risks or gathering social media profile data for generating profiles for contact directories or marketing. (GDPR recital 71 and 91).

Automated decision - making with legal or similar significant effects, a decision about a data subject producing legal effects concerning the natural person made by automated means without any human involvement. An example would be an online decision to award a loan or a recruitment aptitude test that uses pre-programmed algorithms and criteria. (Article 35(3)(a). The processing may lead to the exclusion or discrimination against individuals.

Systematic monitoring – processing used to observe, monitor or control data subjects including through a publicly accessible place on a large scale. For example, using a camera to monitor driving behaviours on a road. (Article 35(3)(c)). The personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used, and it may be impossible for individuals to avoid being subject to such processing in frequent public space.

Sensitive data or data of highly personal nature – this includes special categories of data - racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation, genetic data, biometric data (Article 9) as well as criminal data as defined in Article 10. An example would be a hospital keeping patient medical records or an organisation keeping offender's details. This also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data and financial data. In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by an individual in the course of purely personal or household activity (such as smart technology, cloud computing services for personal

document management, email services, diaries, e-readers equipped with note-taking features and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.

Data processed on a large scale – while the term 'large scale' is not defined, the regulators recommend the following is taken into account: (a) the number of data subjects concerned; (b) the volume and range of data been processed; (c) the duration and permanence of the processing; (d) the geographic extent of the processing activity. (Recital 91)

Datasets have been matched or combined – for example, two or more data processing operations performed for different purposes and/or by different data controllers been combined in way that would exceed reasonable expectation of the data subject.

Data concerning vulnerable data subjects – because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data, e.g. children are considered as not able to knowingly oppose or consent to processing of personal data. Patients, elderly people and asylum seekers would also be considered vulnerable data subjects.

Innovative use or applying technological or organisational solutions – for example combining use of fingerprint and face recognition for improved physical access control, using a video analysis system to single out cars and recognise licence plates. The GDPR makes it clear (Article 35(1) and Recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms.

When processing prevents the data subject from exercising a right or using a service or a contract – for example, processing a public area that people passing cannot avoid or processing that aims to refuse data subjects access to a service or contract (bank screens its customers against a credit reference database in order to decide whether to offer a loan). When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Recital 91). This includes processing performed in a public area that people passing by cannot avoid, or processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

Data transfer across borders outside the EU taking into consideration the envisaged country/ies of destination, the possibility of further transfers.

When is it not necessary to carry out a DPIA?

ETBI Section. are **not** required to carry out a DPIA in the following cases:

- Where the processing is not likely to result in a high risk to the rights and freedoms of individuals.
- Where the nature, scope, context and purposes of the processing are very similar to the processing for which a DPIA has already been carried out.
- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out.
-

Who must carry out the DPIA?

It is the responsibility of the project team (Data Controller) to ensure that a DPIA is carried out for any new project, product, process, system, contract and/or use of end user or employee personal data or changes to existing data processing activities.

How to Conduct a DPIA and What to Include?

Describe the project: Identify the purpose, scope, duration and goals of the project, identify internal and external stakeholders. Include an assessment of the necessity and scale of the processing activity in relation to the purpose. Note the intended outcome for data subjects and the expected benefits for you or for society as a whole.

Describe the envisaged processing - information flows/lifecycle: identify what information is collected, why it is collected, how it is collected, the intended use of the information, with whom the information is shared, the consent and choice rights of the data subjects and how the information will be managed, stored, secured and destroyed. You should provide details of the assets on which personal data rely e.g. hardware, software, networks or paper transmission channels. You may refer to a flow diagram. You should also say how many individuals are likely to be affected by the project and the nature, volume, variety and sensitivity of the personal data including information on whether the data subjects include children or other vulnerable people.

You should identify the legitimate interest in carrying out the processing.

When codes of conduct (outlined in the GDPR) are put in place, the description of processing will have to include measures taken to comply with these codes of conduct and period for which the personal data will be stored.

Consider the following:

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Consult with Stakeholders

You should seek the views of data subjects (or their representatives) unless there is a good reason not to. In most cases it should be possible to consult individuals in some form, e.g. internal stakeholders such as project management team, IT, procurement, potential suppliers (processors), communications teams, customer facing roles, researchers, senior management and then external stakeholders including people who will be affected by the project and members of the public.

However, if you decide that it is not appropriate to consult individuals then you should record this decision as part of your DPIA, with a clear explanation, e.g. you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers the processing of personal data of existing contacts e.g. employees, you should design a consultation process to seek the views of those particular individuals or their representatives.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process or targeted research. If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.

If you use a data processor, you may need to ask them for information and assistance.

Assess Necessity and Proportionality:

You should consider -

Do your plans help to achieve your purpose?

Is there any other reasonable way to achieve the same result? your lawful basis for the processing, how you will prevent function creep i.e. using the data for more than the original purpose, how you intend to ensure data quality, how you intend to ensure data minimisation, how you intend to provide privacy information to individuals, how you implement and support individual's rights, measures to ensure your processors comply and safeguards for international transfers.

Identify and Assess Risks:

Identify the key privacy risks to the data subjects and the associated compliance and corporate risks, giving consideration to the likelihood and severity of the risk and the impact of the risk. Conduct a check against legal, regulatory, industry and organisational standards. Each Functional area are required to document the risks involved in the processing and identify the likelihood and severity of the identified risk (assessment of risks).

Evaluate how information handling practices at each stage of the project may affect privacy as well as the potential impact on individuals and any harm or damage that might be caused by your processing, whether physical, emotional or material. In particular, look at whether the processing could possibly contribute to:

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach including illegitimate access to, modification of or loss of personal data.

Having identified the risks, it is then necessary to assess which are going to pose the greatest threat by looking at both the likelihood of the risk occurring and the impact that might result. This provides the overall risk rating.

Identify privacy solutions and controls to reduce or eliminate the risks: identify appropriate measures in place to address and mitigate risks, identify alternatives to collection and handling processes, identify appropriate technical controls to mitigate privacy risks e.g. encryption, relevant security measures. Describe organisational measures e.g. robust policies staff training, etc. Describe the actions you could take to reduce the risks and any future steps which would be necessary. Functional Area are required to assess whether the impact on privacy is necessary and proportionate to the outcomes of the new product, process, system, contract, and/or use of end user or employee personal data (assessment of the necessity and proportionality).

See the Chart below for examples of actions you could take to reduce the impact/likelihood and mitigate the risk.

Document the Results / Signing off on the outcomes of the DPIA: ensure appropriate sign off of outcomes is formally documented and retained.

Record what additional measures you plan to take, whether each risk has been eliminated, reduced or accepted, the overall level of 'residual risk' after taking additional measures and whether the Data Protection Commission needs to be consulted.

You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. However, if there is still a high risk, you need to contact the Information & Compliance Officer and/or DPO who will consult with the Data Commissioner before you can go ahead with the processing. As part of the sign-off process, you should ask the Information & Compliance Officer to advise on whether the processing is compliant and can go ahead. If you decide not to follow their advice, you need to record your reasons. You should also record any reasons for going against the views of individuals or other consultees.

Implement and Review – You must integrate the outcomes of your DPIA i.e. the data protection solutions, back into your project plans. Create a summary describing the rationale for the final design choice or business process, ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld. If appropriate, publish the summary to provide transparency and accountability. This could help foster trust in your processing activities and improve individuals' ability to exercise their rights by explaining the reasoning behind the design of systems and how they are engineered with privacy considerations in mind.

You should identify any action points and who is responsible for implementing them. You should monitor the ongoing performance of the DPIA. **On-going management of a DPIA**

The DPIA must be a living document throughout the lifecycle of the processing and each Functional area must ensure that it is kept up to date at all times. The revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over longer time. Where necessary, the relevant line manager will conduct a review to assess if processing is performed in accordance with the DPIA at least when there is a change of the risk represented by processing operations e.g. where a significant change to the processing operation has taken place in terms of context, risks, purposes, personal data processed, recipients, data combinations, security measures and/or international transfers.

Where necessary, the Information & Compliance Officer and/or Director of OSD may also independently conduct a review to assess if processing is performed in accordance with the DPIA.

Consultation - Please note where the output of a DPIA indicates that the processing involves a high risk which a Functional Area cannot mitigate or which the costs of mitigation are too high, the line manager is required, with the input of the Information & Compliance Officer and DPO, to consult with the Office of the Data Protection Commissioner prior to commencing the processing.

Appendix G - Information Guidance on risk and solutions

Example of Risks to Individuals:

- Inappropriate disclosure of personal data internally due to a lack of appropriate controls being in place.
- Data may be kept longer than required in the absence of appropriate policies.
- Loss of confidentiality, e.g. accidental loss of electronic equipment may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Discrimination, e.g. vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Re-identification of pseudonymised data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Loss of control over the use of their personal data, e.g. being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals and may inadvertently allow individuals to be identified from anonymised data.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.
- inability to exercise rights
- inability to access services or opportunities
- identity theft or fraud
- financial loss
- reputational damage
- physical harm
- any other significant economic or social disadvantage.

Examples of Corporate Risks.

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.

- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of organisation's use of personal information may lead to a reluctance on the part of individuals to deal with the organisation.
- Problems with project design identified late in the design process or after completion, may be expensive and cumbersome to fix.
- Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.
- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the organisation. Under the GDPR, ETBI may also be liable for non-material damage.

Examples of Compliance Risks:

- The organisation may face risks of prosecution, significant financial penalties, or reputational damage if it fails to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.
- Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Examples of data protection solutions (measures to address risks):

- Deciding not to collect or store particular types of information.
- Reducing the scope of the processing
- Devising strict retention periods, designed to minimise the length of time that personal data is retained.
- Planning secure destruction of information.
- Ensuring that staff are properly trained and are aware of potential privacy risks to ensure risks are anticipated and managed.
- Creating internal guidance and protocols for information handling within the project.
- Producing guidance for staff on how to use new systems, as a reference point in the event of any uncertainty relating to the handling of information and how to share data if appropriate.
- Making changes to Privacy Notices and Records of Processing Activities.
- Implementing appropriate and/or additional technological security measures.
- Consider using a different technology.

- Assessing the need for new IT systems to safely process and store the data and providing staff with training in any new system adopted.
- Assessing the possibility of using anonymised or pseudonymised data as part of the project to reduce identification risks.
- Ensuring that data subjects are fully informed about how their information will be used if appropriate.
- Offering data subjects the chance to opt out where appropriate.
- Providing a contact point for individuals to raise any concerns they may have with the organisation.
- Implementing new systems to help individuals to exercise their rights.
- Adding a human element to review automated decisions.
- If using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements (Data Sharing Agreements) to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks. You should ask for advice.

Appendix H - Record of Processing Activities (ROPA) under GDPR Article 30

Revision History

Date of this revision:	Date of next review

Version No. / Revision No.	Revision Date	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date

This Policy shall be reviewed and, as necessary, amended by ETBI annually. All amendments shall be recorded on the revision history section above.

1. Data Controller Details

Name: Education and Training Boards Ireland

Address: Piper's Hill, Naas, Co Kildare, W91K729

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Telephone Number: +353 (0)45-901070

2. Categories of Data Subjects

ETBI collects personal data from the following categories of data subjects:

- Current Employees, prospective employees, former employees
- External Examiners
- Family members – children\dependents in cases of parental leave,
- HR Recruitment panel members
- Professional Advisors, Consultants and Contractors, Creditors
- ETBI's Governing Body and FAR Committee members
- Members of public including visitors or those using services or facilities

More rarely, and on case-by-case basis, additional processing may take place involving following categories of data subjects -

Subjects involved in complaints or investigations by regulatory or law enforcement authorities, including CCTV footage of particular events or data processed through security systems.

Individuals involved in any accidents or incidents including involvement of Emergency Services.

Details of persons involved in or affected by data incidents (which may contain personal data).

Persons involved in legal or insurance claims involving ETBI.

Categories of Personal Data

ETBI collects the following categories of personal data:

3.1 Relating to Human Resources (HR) Functions

- Details of Candidates not qualified or shortlisted
- Unsuccessful Candidates who are Shortlisted or called for Interview
- Applications and CVs of Candidates who are called for interview

- Interview Evaluation Sheet
- Interview Board Interview Notes
- Selection Board Report and other Interview Documentation
- Application/CV of successful candidate
- Pre-Employment medical reports
- Employment Contract
- Probation forms
- Leave Records (paid and unpaid)
- Time & Attendance Records
- Personal Development forms
- Copy of birth certificate/Passport (not currently collected)
- Unpaid Absence records
- Transferred Service
- Pre entry / transferred service information
- Case Management Files
- Records of formal meetings with staff created by Centre Managers and where HR do not have the originals

Special categories of personal data may be included in the following:

- Health data for purposes of disability support/employment purposes, occupational health and/or public health (Covid-19 Return to work form)
- Grievance, disciplinary, fitness to practice or HR attendance record data.
- Performance information
- Offences and alleged offences
- Information on Criminal conviction for vetting purposes
- Racial or ethnic origins
- Trade union membership
- Visa and immigration details

For purposes of Equality, Inclusion and Diversity (voluntary):

- Gender
- Gender Identity
- Age
- Nationality
- Disability
- Racial origin/ethnicity

- Civil Status

3.3 Relating to Service Provisions including Estates and ICT

ICT Domain accounts for staff and user-generated content on home folders located on ETBI storage area networks (SAN) .

Google G-Suite and Office 365 accounts for staff and user-generated content on personally assigned home folders

Data backup operations (email)

Monitoring logs - RMS

Support requests

CCTV and Printing

3.4 Relating to contractual and financial functions e.g. administering payments/fees/research funding:

Financial details of individuals both Creditors and Debtors of ETBI - Staff Bank Details

ROS (Revenue Commissioners) tax information for employees

Social Welfare information for employees

Staff Pay Claims

Travel and Subsistence Claims

3.5 Relating to compliance; prevention and detection of crime, safety, security, accident/ incident management and legal/insurance claims

Professional Advice & Related Correspondence – Professional advice and briefings/ correspondence on employment and public liability matters

Insurance –Insurance Claims by staff /member of the public.

ETBI Governing Body Meeting Records – Agendas, minutes, tabled documents, Reports, Attendance Sheets, Correspondence to/from Governing Body, etc.

Standards in Public Office (SIPO) Records – Annual SIPO Returns-Statements of Interest.

External Work Declarations.

4. Purposes of Data Processing

ETBI obtains, processes, collects, keeps, uses, discloses (where permissible by law), and retains Personal Data and/or Special Categories of Personal Data regarding its staff, service users and other individuals who come in contact with, avail of the services of or engage in business with ETBI.

The purpose of processing Personal Data and Special Categories of Personal Data include but are not limited to:

- fulfilling ETBI's functions and obligations and ETBI policies and procedures
- undertaking of research activities
- the recruitment and employment of staff
- compliance with statutory obligations
- reporting to Government and regulatory bodies
- the provision of commercial activities
- the management of financial affairs
- the provision of information solutions and services
- the provision of library services
- advertising and promoting ETBI
- undertaking fundraising by or on behalf of ETBI
- Public health (such as Covid-19)

ETBI also processes personal information through CCTV systems that monitor and collect visual images for the purposes of security and the prevention and detection of crime and offences.

These activities are carried out on behalf of ETBI by its functional area. In some cases, more details are available through the Functional area Records of Processing Activity (e.g. Data Inventories) and/or Data Protection Notices.

5. Categories of Personal Data Recipients (Third Parties)

Information relating to staff may be shared with:

The Department of Education and Skills (DoES)

The Department of Public Expenditure and Reform (DPER)

The Department of Social Protection (DSP)

The Higher Education Authority (HEA)

Quality and Qualifications Ireland (QQI)

The Comptroller and Auditor General (CAG)

The Revenue Commissioners

The Health Service Executive (HSE)

The Office of the Ombudsman

The Office of the Information Commissioner (OIC)

The Office of the Data Protection Commissioner (DPC)

The Workplace Relations Commission (WRC)

Interview Assessment Boards

Governing Body Members

Referees

Pension Scheme Administrators for operation of pensions relating to employees.

Nominated Occupational Health Provider:

Transfer of leave and pension records for staff who are taking up new employment outside ETBI (if requested by the employee)

Transfer of leave and pension records for staff who are taking up new employment outside ETBI (if requested by Employee)

Research Funding Bodies

IT and Other Service providers who act as our processors when carrying out ETBI's functions.

Banks to facilitate EFT transfers

Insurance, legal advisors, third party investigators, Workplace Relation Commission

Transfer of leave records to new employer

Online application for Tax Saver incentive scheme

Legal advisors, third party investigators

Internal Auditors

Research Funding Auditors

European Community Auditors

Other regulatory bodies, where required to do so

This is not an exhaustive list and other disclosures to third parties not listed here are made only where we consider it is lawful to do so.

European Economic Area / Overseas

For those employees who are involved with one of our overseas partners, or who have funding sponsors or guarantors, or other nominated contacts, who are based outside of the EEA or those who are working with entities belonging to ETBI group or partners of ETBI based outside the EEA, some information may be transferred to those other locations.

Where personal data are transferred to partners outside the EEA ETBI will put in place Data Processing Agreements, using the Standard Contractual Clauses as approved by the European Commission, and take steps to ensure that appropriate security and privacy measures are taken with the aim of making sure that data subject privacy rights continue to be protected.

6. Personal Data Retention Periods

Except as otherwise permitted or required by applicable law or regulation, ETBI aims to retain personal data for only as long as is necessary to fulfil the purposes ETBI collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for personal data, ETBI will consider the amount, nature, and sensitivity of personal data, the potential risk of harm from unauthorized use or disclosure of personal data, the purposes for processing the personal data, whether the employer can fulfil the purposes of processing by other means, and any applicable legal requirements. **7. Changes to this document**

ETBI reserves the right to amend this record of processing activity from time to time consistent with the GDPR and other applicable data protection requirements and to reflect changes in the organisation over time.

Appendix J - Subject Access Request Form

Data Subject Access Request Form: Request for a copy of Personal Data under the Data Protection Acts 1988 to 2018 and under Article 15 of the General Data Protection Regulations 2016/679

1. Details of Requester

Surname: _____

First Name: _____

Email Address: _____

Postal Address: _____

_____

Telephone number: _____

If you are a current or former staff member, please provide details of the Section:
_____

If you are not a staff member, please provide details of your relationship with ETBI:

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

_____
_

2. Form of Access

My preferred form is access is:

To receive photocopies by post: ☐ To receive soft copy by email: ☐

To receive photocopies by hand: ☐ Other, please detail: _____

3. Details of Request

I, _____ , wish to have access to data that I believe ETBI retains on me as outlined above.

I acknowledge that, before I am given access to personal information about myself, I may be asked for ID.

Signed: _____ **Date:** _____

Please return the completed forms together with a copy of proof of identity to:	**By post to:** ETBI Education and Training Boards Ireland, Piper's Hill, Naas, Co Kildare, W91K729

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

	Or by email to james.eustace@etbi.ie

For ETBI office use only:

Reference No: _____
Date Received: _____
Date of acknowledgement to requester: _____
Identity verified: _____
Identification securely destroyed (Y / N): _____
Date of response issued to requester: _____

Appendix J - Subject Rights Request Form

Data Subject Rights Request Form (SRR)

Request for Rectification / Erasure / Restriction of Processing of Personal Data /Objection to Marketing

under the Data Protection Act 2018 and under the General Data Protection Regulations 2016/679

1. Details of Requester (Please use block capitals when completing form)

Surname:

_____

First Name:

_____

Email Address:

_____

Postal Address:

_____

_____

Telephone number: _____

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

2. Your relationship with ETBI

If you are a current or former **staff member**, please provide:

- your Staff ID Number: _____

- details of the Section/ Office: _____

If you are not staff member, please provide details/dates of your relationship with ETBI:

_____

_____

_____

3. Data Subjects Rights Request

In the box below, please tick which type of Data Subject Right you wish to exercise.

- Rectification of Personal Data – Article 16
- Erasure of Personal Data /Right to be Forgotten – Article 17
- Restriction on Processing of your Personal Data – Article 18
- For right to Data Portability – Article 20
- Objection to Marketing – Article 21

4. Details of your Data Subject Rights Request

Please tick one box below:

- Your personal data held by ETBI be amended - Article 16
- I request that ETBI erase my personal data - Article 17
- I request that ETBI restrict the processing of my personal data for one of the following three reasons:
- I wish to contest the accuracy of my personal data and to have the processing of this data restricted whilst ETBI verify the accuracy of the data - Article 18 1 (a)
- I think the processing of my personal data is unlawful - Article 18 1 (b)
- ETBI no longer needs my data for the purposes of its processing, but it is required by me for the establishment, exercise or defence of legal claims - Article 18 1 (c)
- I object to ETBI contacting me for marketing purposes - Article 21

For requests under Article 20 – Right to Data Portability - please provide details of your request

5. Identification and Verification

In order for ETBI to protect the security of personal data, it is necessary for you to provide proof of your identity.

A copy of your ID must accompany this form before your request can be processed.

Copies are acceptable in most cases. However, ETBI reserves the right to ask to see original documents where necessary. Copies of such documents sent with this form will be securely destroyed once we have verified your identity.

Please complete *either* section 6 *or* section 7

6. Declaration of Data Subject

I confirm that I am the Data Subject named in Section 1 and I am making this request for the rectification/erasure/restriction of processing my personal data/objection to marketing. I understand that the information I have supplied will be used to confirm my identity and help locate the data I am referring to.

Signed: _____ **Date:** _____

or

7. Declaration of Data Subject for Agent to act on their behalf

If you wish someone else to submit a Data Subject Rights Request on your behalf (e.g. family member, solicitor) please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my data request. I have enclosed evidence of my identity referred to in Section 5 and confirm that I want all correspondence and responses to my request to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and locate the data I am referring to.
Signed: _____ **Date:** _____
Name of Agent: _____
Relationship to Data Subject:_____
Address: _____
Telephone Number: _____

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Email address: _____

Returning your completed form:

Please return the completed form together with a copy of proof of identity to:	**By post to:** **ETBI** Education and Training Boards Ireland, Piper's Hill, Naas, Co Kildare, W91K729 **Or by email to** james.eustace@etbi.ie

For ETBI office use only:

Reference No: _____
Date Received: _____
Date of acknowledgement to requester: _____
Identity verified: _____
Identification securely destroyed (Y / N): _____
Date of response issued to requester: _____

Appendix K - Procedure for reporting personal data breaches

Under Article 33 GDPR ETBI must report a data breach, if deemed reportable, to the Data Protection Commission within 72 hours of becoming aware of the breach. This timeframe includes weekends and bank holidays.

Under Article 34 GDPR ETBI must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy.

As such, any data breach must be dealt with immediately and appropriately. If a member of ETBI becomes aware of an actual, potential or suspected data breach, they must report the incident to their line manager/Directorate immediately. The line manager/Directorate must then immediately report the incident to the Director of Organisation Service (OSD) and Development. Early recognition and reporting is vital to ensure the breach can be dealt with swiftly and appropriately.

After reporting the incident, the relevant member of ETBI must complete the Personal Data Breach Report Form (*see Appendix 1 below*) and forward it to the Director of OSD as soon as possible. The Director of OSD and/or HR/IR Governance Officer is responsible for keeping a written record of all potential or suspected data breaches that are notified to them (including those that are not notified to the Data Protection

Commission or the affected individuals). For this purpose, it is imperative that the Personal Data Breach Report Form is completed satisfactorily. This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

Procedure for managing personal data breaches

Upon receiving notification of a data breach, the Director of OSD shall, in conjunction with appropriate members of staff, take the following five steps (in line with best practice) when responding to the incident:

Step 1: Identification and initial assessment of the incident Step 2: Containment & recovery Step 3: Risk assessment Step 4: Notification Step 5: Evaluation & response

Step 1: Identification & initial assessment of the incident

If any member of ETBI considers that a data breach has, or might have, occurred, they must report the incident immediately and complete the Personal Data Breach Notification form.

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

The Personal Data Breach Notification Form will assist the Director of OSD in conducting an initial assessment of the incident.

This assessment will take into account:

- Whether a data breach has taken place
- The nature of the personal data involved in the breach (i.e. whether sensitive or confidential personal data is involved)
- The cause of the breach
- The extent of the breach (i.e. the number of individuals affected)
- The potential harms to which affected individuals may be exposed - Any steps that may be taken to contain the breach

Following this initial assessment of the incident, the Director of OSD may, according to the severity of the incident, consult with the LSSU and decide if it is necessary to appoint a group of relevant ETBI stakeholders (e.g. IT Services, Human Resources, FET, Schools, OSD & Change Programme Manager) to assist with the investigation and containment process.

Step 2: Containment & recovery

In the event of a data breach, immediate and appropriate steps must be taken to limit the extent of the breach.

The Director of OSD, in consultation with relevant staff, will:

- Establish who within ETBI needs to be made aware of the breach (e.g. IT Services, Communications Office) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network)
- Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach
- Where appropriate, inform the Gardaí (e.g. in cases involving criminal activity)

Step 3: Risk assessment

The Director of OSD, in conjunction with relevant staff, will use the information provided in the Personal Data Breach Notification Form to fulfil the requirement to assess the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as no risk / low risk / medium risk / high risk in accordance with the detailed criteria below:

a) Type of breach: A data breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of personal data. What type of data breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to personal data? Is there a temporary or permanent lack of availability or access to personal data and if temporary, how long will it be before it is restored?

b) Nature of personal data: Is the relevant personal data sensitive in nature? The more sensitive the personal data the higher the risk of the data breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.

c) Scale and volume of personal data affected: The higher the volume of the personal data records and the number of individuals potentially affected will usually create a higher risk.

d) Ease of identification: The ease of identifying the relevant individuals based on the personal data will likely increase the risk of identity theft, fraud and reputational damage in particular.

e) Security measures: Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact, and the data is unintelligible to a third party?

f) Containment measures: Have any containment measures been implemented which mean that the data breach is unlikely to present a risk to the individuals affected?

g) Other factors: Other relevant factors in assessing the risk to individuals is whether those individuals affected by the data breach have any special characteristics (for example children or vulnerable adults).

h) Severity of risk: Based on the above criteria and any other relevant factors, the Director of OSD should assess the severity of the risk in terms of the potential consequences to the individuals affected by the data breach.

i) Likelihood of the risk(s) materialising: Once the data breach has occurred, the Director of OSD must objectively assess the likelihood of the potential risks actually materialising and this should form part of the risk assessment.

An assessment of the risks for ETBI, including strategic and operational, legal, financial and reputational risks may also be prepared.

Step 4: Notification

Data Protection Commission: Under Article 33 GDPR ETBI must report a data breach, if deemed reportable, to the Data Protection Commission within **72 hours** of becoming aware of the breach. This timeframe includes weekends and bank holidays.

If the relevant details surrounding the data breach are not clear within the initial 72-hour notification period, an initial notification should be made to the Data Protection Commission. Subsequent notifications can be made to the Data Protection Commission in phases. Consideration as to whether a communication to affected individuals is required should be addressed when notifying the Data Protection Commission.

All contact with the Data Protection Commission should be made through the Director of OSD.

The decision to report a breach to the Data Protection Commission will ultimately be made by the Director of OSD, in consultation with the relevant the General Secretary and Executive Leadership Team.

Affected individuals: Under Article 34 GDPR ETBI must inform affected individuals without undue delay, if the data breach is likely to result in a high risk to their privacy.

Where the Director of OSD assesses that there is a high risk to rights and freedoms of individuals as a result of the data breach, then the existence of the data breach should be communicated to the affected individuals **without undue delay**.

Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the data breach. The Director of OSD should determine the most appropriate and effective means of communicating the data breach to the affected individuals, if necessary, engaging the assistance of communications advisors.

Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

In each case, the notification should include as a minimum:

- a description of the nature of the breach;
- a description of the likely consequences of the breach;
- how and when the breach occurred;
- what data was involved;

- a description of the measures taken or proposed to be taken by ETBI to address the breach; - the name and contact details of the Director of OSDr and other contact points.

Other parties: ETBI should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí, insurers, external legal advisers etc.).

Step 5: Evaluation & response

Certain data breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the data breach, its causes, and likely consequences, in order to effectively contain the breach. The effect of the data breach must be monitored, and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification program with the Data Protection Commission in these instances.

In the aftermath of a data breach, a post-incident review of the incident should take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any area that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise, in order to reduce the recurrence of similar data breaches and to ensure that appropriate technical and organisational security measures are put in place.

Guidance

For further information and advice about what to do in the event of a suspected data breach please contact:

Line manager

Or by post to

ETBI - Education and Training Boards Ireland, Piper's Hill, Naas, Co Kildare, W91K729 **Or by email to**

james.eustace@etbi.ie

Appendix L - Personal Data Breach Notification Form

Data Breach Incident Notification – Instructions for Completion

If you discover a personal data security breach, please notify your line manager immediately.

Please complete the Data Breach Incident Notification and return it to the Director of Organisation Support & Development **as soon as possible** **james.eustace@etbi.ie** Please note that there is a very short period of time in which to notify the Data Protection Commissioner – 72 hours.

Please refer to Terms and Definitions for clarification on the data protection terminology used in some questions.

If you require assistance, please do not hesitate to contact
ETBI's General Secretary ETBI's HR/IR Governance Officer

Data Breach Incident Notification

Initial Incident Report ***(To be completed by individual reporting the incident and/or Manager)***	
Name:	Function:
Date:	Staff Number:
Location:	
Date of Incident:	Time of Incident:

Document Reference Number	COR008 Data Protection Policy
Implementation Date	**01st January 2022**
Review Date	31st January 2024
Next Review Date	31st January 2024
DES Circular Letter	Data Protection Acts 1988 to 201 General Data Protection Regulation 2016/67
Governing Body Approved	25th January 2022

Who was Notified?	Data and Time of Notification:
Description of Incident:	
Type of breach: Confidentiality breach, Integrity breach, Availability breach	
Estimated number of Data Subjects affected	
Estimated number of records affected	
Categories of Data Subject affected (e.g. employees, the public, suppliers etc.)	
Categories of personal data affected (e.g. Contact Details, Health Data, Bank Details, etc.)	
Any Sensitive Category personal data? (E.g. Health, Trade Union Membership, Ethnic Origin, etc.) Y/ N	
What device or system was the personal data held on?	

Are there any reasons to suspect that the passwords used to protect the personal data may have been compromised? (e.g. password stored with mobile device or weak password used)	
Any further information:	
Signed By individual reporting incident:	**Date:**
Signed By Manager:	**Date:**

Data Breach Incident Notification – Terms and Definitions

Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by ETBI. Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of or an employee HR file • Notes of personal supervision, including matters of behaviour and discipline.

Personal Data Breach	GDPR defines a "personal data breach" as: *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*
Breach Incident	A breach incident includes but is not restricted to the following: • **Unauthorised disclosure** of personal data (this includes disclosure to recipients that are not authorized to receive the data) • **Loss** or theft of confidential or sensitive personal data or the equipment used to store the data (e.g. laptop, USB key, tablet, paper record) • **Accidental or unlawful destruction** (e.g. failure of equipment) • Unauthorised use of access to or **modification/alteration** of personal data or IT systems • Attempts to gain unauthorised access to information or IT systems • Human error **Destruction –** where the data no longer exists, or no longer exists in a form that is of any use to the Data Controller. **Damage –** where personal data has been altered, corrupted, or is no longer complete. **Loss –** where the data may still exist, but the Data Controller has lost control of or access to it, or no longer has it in its possession.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.
Data Subject	Refers to the individual to whom Personal Data held relates, including employees, customers, suppliers.

Types of Breach	**Confidentiality Breach** – where personal data is disclosed or accessed in an unauthorised or accidental manner. **Integrity Breach** – where personal data is altered in an unauthorised or accidental manner. **Availability Breach** – where personal data is lost or destroyed in an unauthorised or accidental manner.
Unauthorised or unlawful processing	This may include disclosure of personal data to (or access by) recipients who are not authorised or do not have a lawful basis to have access to the personal data.