Institute of Technology Tallaght

Data Protection Policy

Version 1.0

Document Location

To be completed by Data Protection Officer

Revision History

Date of this revision:	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date
SMT	Senior Management Team	6 June 2018
AC	Audit Committee of Governing Body	8 June 2018
GB	Governing Body	13 June 2018

This Policy was agreed by the Governing Body on 13th June 2018. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1. POLICY

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

The Institute as a Data Controller, has established this 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 the Institute's policy regarding Personal Data collection/processing/sharing for all Schools and Functions, staff and students.

The Institute 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 the Institute's competence and confidentiality while handling data.

This policy should not be viewed in isolation. Rather, it should be considered as part of the Institute of Technology Tallaght suite of Data Protection policies and procedures (see GDPR Common Definitions & Terms Policy)

2.PERSONAL DATA

2.1 Personal Data Processing Principles

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

The Institute 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 for 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)

The Institute 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)

2.2 Personal Data Processing Policy Requirements

The Institute 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.

Only Data Protection Oversight Committee approval may allow Data Processing in the absence of one of these conditions.

Consent

For Processing based on Consent, Schools and Functions 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. This includes Data Aggregation activity either for Institute use or by Third Parties on behalf of the Institute.

In particular, Data Processing Consent cannot be implied and must be:
- Freely given
- Specific
- Informed
- Unambiguous
- Provided by an affirmative action (Opt-in as opposed to Opt-out)

Appropriate Consent Request methods include:
- Clauses in contracts with students and vendors, and / or
- Check boxes on replies to applications or forms, and / or
- Click boxes on online forms where Personal Data is entered

Any Consent Request (written) must be:
- Clearly distinguishable from other matters
- Presented in clear and plain language

All Schools and Functions 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 disclosures must be made in order to obtain a valid Consent,

- documentation of the date,
- method and content of the disclosures made,and
- validity, scope, and volition of the Consents given.

All Schools and Functions shall establish Consent Withdrawal processes and inform Data Subjects about:

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

Special Categories Personal Data Processing

The Institute will not process Special Categories of Personal Data unless;

- The Data Subject expressly Consents
  and / or
- 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
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

The Institute may only process such data where 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 the Data Protection Officer 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 the Data Protection Officer (DPO) in consultation with the Data Protection Oversight Committee.

Refer to Appendix B for an example of a Privacy Notice requirements checklist.

2.3 Procedures at the Time of Collection of Personal Data

To ensure fair and transparent processing activities Schools and Functions must provide fair disclosure notices to Data Subjects when directly collecting data.

These disclosures 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 the Disclosure.

If Schools and Functions use Consent as the Processing Personal Data condition then this Processing Consent must be obtained at data collection point.

All Schools and Functions collecting Personal Data must establish technical or administrative means to:

- Deliver the fair disclosure notice, and

- Document that the Institute has provided a fair disclosure notice to the Data Subject at the time of collection, or document that the fair disclosure notice was previously provided, and
- Record all obtained Consents and ensure this information is up to date.

Schools and Functions must provide all of the following to Data Subjects in the form of a fair disclosure notice at Personal Data collection point of:

- Data Controller's (DPO) name and business address.
- Information Collection purpose.
- Information processing legal basis.
- Identities/Categories of all natural/legal persons to whom the Data controller could or may send Personal Data. (Joint Data Controllers or other Data Processors)
- Whether the Institute will or could transfer Personal Data outside of the European Economic Area and if the EU Commission has determined if the recipient jurisdiction/country has adequate Data Protection laws in place.
- The information transfer terms i.e. pursuant to a contract including EU Commission's Model Contractual Clauses, or other legally approved mechanism.
- Notice of the Data Subject's various GDPR rights including access rights, rectification, erasure, correction, restriction on processing, objection and portability of Personal Data held about them, and the means of exercising those rights (for example, who to contact).
- How long the Institute expects or intends retaining the Personal Data.
- Notice of the Data Subject's right to lodge a complaint with the supervisory authority and the Institute's lead supervisory authority details.
- Notice of statutory or contractual requirements underpinning this Personal Data provision request.
- Notice of whether the data subject is obliged to provide the Personal Data and the consequences of not providing the Personal Data.
- If Processing involves automatic decision making or profiling than the notice should provide meaningful information about the automatic decision making logic and consequences of the Processing for the Data Subject.
- Any other information to guarantee "fair processing", as deemed necessary by the School or Function in consultation with the DPO. For example, the Institute should disclose where it may use the Personal Data in a manner not apparent to the Data Subject.

If the School or Function 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 fair disclosure notice.

Wherever possible, these disclosures 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 DPO in consultation with the Data Protection Oversight Committee. In the case of employees, the disclosures should be made in the employment contract. Appropriate disclosures should also be made in any job application form, employee handbook or other internal employment document. The disclosures should be made in a manner calculated to draw attention to them.

The fair disclosure notices content and mechanism requires prior DPO approval in consultation with the head of School or Function.

2.4 Personal Data Sources

In contrast to Section 2.2 above, when the Institute collects Personal Data from a Third Party (i.e. not directly from a Data Subject), the Data Controller must provide "Fair Disclosure 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.

School and Functions may not disclose Personal Data to Third Parties prior to informing the Data Subject of their rights. In addition to the fair disclosure notice content outlined in Section 2.3 of this Policy, the Data Controller shall provide the Data Subject with the following information necessary to ensure fair and transparent Processing of their Personal Data:

- The Personal Data collection and whether this was a public source.
- The Personal Data categories concerned.

The following are the only exceptions:

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

2.5 Data Minimisation

School and Functions should limit Personal Data collection to:

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

School and Functions 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.

2.6 Data Use Limitation

School and Functions must only collect Personal Data for specified, explicit and legitimate purposes. They are prohibited from further Processing unless they have identified legitimate Processing conditions and documented same as per Section 2.2 of this policy or if the Personal Data involved is appropriately Anonymised and / or Pseudonymised and used for statistical purposes only.

2.7 Data Accuracy

Each School and Function must ensure that any collected Personal data is complete and accurate subject to limitations imposed by Institute/ Third Party contractual provisions.

In addition, each School and Function must maintain Personal Data in an accurate, complete and up-to-date form as its purpose requires. Furthermore they shall correct incorrect, inaccurate, incomplete, ambiguous, misleading or outdated information without prejudice to:

- Fraud prevention based on historical record preservation.

- Legal Claim establishment, exercise or defense.
- Document Retention policy or other internal procedure.

2.8 Data Storage Limitation

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

School and Functions should erase any Personal Data that violates:

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy
- If the Institute no longer requires the Data
- If the Personal Data no longer benefits the Data Subject in the relevant process

School and Functions should Anonymise and / or Pseudonymise Personal Data 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, the Institute disagrees with that assertion and resolution has not been reached.

2.9 Integrity and Confidentiality of Personal Data

Information Security

Each School and Function shall ensure Personal Data security through appropriate physical, technical and organisational measures. These security measures should prevent:

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

When implementing Personal Data security measures each School and Function must consider:

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

IT management must adequately relate EU Data Protection requirements to relevant Institute IT Policies, Procedures and Programs.

Protect Institute and Confidential Information Privacy

European Data Protection requirements specifically refer to Personal Data collected and Processed within Europe. However, the Institute is committed to protecting all collected, processed, stored and transferred (strictly) confidential information regardless of country of origin.

Unauthorised Disclosure

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

Staff must report all suspected incidents of unauthorised access to the DPO. Incidents include disclosure, loss, destruction or alteration of (strictly) confidential information, regardless of whether it is in paper or electronic form. Schools and Functions must establish formal procedures and a point of contact to report all potential unauthorised disclosure incidents.

2.10 Privacy by Design, Data Protection by Design and Data Protection by Default

The Institute aims to ensure that Data Protection and Privacy impacts are fundamental to all processes. Aside from general Data Protection policy, School and Functions must incorporate the following principles when designing or changing a service/project:

- Privacy by Design and by Default
- Data Protection by Design and by Default

If the School and Function considers that particular Personal Data Processing may affect a Data Subjects rights and freedoms than they should:

- Engage the DPO in terms of the issue.
- Conduct a Data Protection Impact Assessment (DPIA).

School and Functions 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 and any specific guidelines and requirements set by the DPO, or IT Policies in furtherance of these principles.

When the Processing of Personal Data may result in a high risk to the rights and freedoms of a Data Subject, School and Functions are required to conduct a Data Protection Impact Assessment (DPIA) and then consult with the DPO. Where requirements have not been established, or where there is any confusion as to the applicability of Data Protection requirements, referral must be made to the DPO and the Privacy by Design principles, set out in the Systems Development Life Cycle Policy (Privacy by Design by Default). *NOTE: The Systems Development Life Cycle Policy has not yet been approved.*

Refer to Appendix C for a Data Protection Impact Assessment Examplar.

2.11 Data Processing Activity Inventory

Each School and Function must maintain a written record of processing activity under its responsibility.

When Operating as a Data Controller

When operating as a Data Controller, each School and Function must maintain a written record of processing activities to include:

- Data Controller name and contact details (and joint controller if applicable), the Data Controller's representative and the DPO
- The Processing purposes
- Data Subjects category description
- Personal Data category description
- Personal Data disclosure recipient categories
- If outside the European Economic Area, the recipient identification, country and Personal Data protection relevant transfer mechanisms and safeguards
- Personal Data erasure time limits by category
- Personal Data safeguarding technical and organisational security measures

When Operating as a Data Processor

When operating as a Data Processor, each School and Function must maintain a Processing activity written record when carried out on a Data Controllers behalf for the Processing relationship lifetime. That record must, at a minimum, retain the following information:

- Data Processor name and contact details and of each Data Controller which the Data Processor is acting on behalf of
- Data Processor's representative name and contact details, the Data Controller's representative, and the DPO
- The Processing categories carried out on behalf of each Data Controller
- If outside the European Economic Area, the recipient identification, country and Personal Data protection relevant transfer mechanisms and safeguards
- Personal Data safeguarding technical and organisational security measures

Data Processing Activity Inventory Maintenance

School and Functions must maintain all completed processing activity records on a system accessible to the DPO. The DPO will review these records periodically and will update same accordingly, in consultation with the Data Controller. The DPO will provide Processing Activity records to a supervisory authority on request.

Refer to Appendix A for a template for documenting the Data Processing register.

2.12 Third Party Transfer

School and Functions must not transfer Personal Data to a Third Party outside of the EEA regardless of whether the Institute is acting as a Data Controller or Data Processor unless:

- The EU recognises the transfer country/territory as having an adequate level of Data Subject legal protection relating to Personal Data Processing or
- The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection.
- The original Personal Data consent explicitly allows Third Party transfer or transfer is authorised by law.
- All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal Data Protection; and
- The Institute has received legal advice that necessary contractual provisions support the transfer.

Subject to the provisions above, including any necessary Institute approvals, School and Functions may transfer Personal Data to a Third Party outside of the EEA where any of the following apply:

- The Data Subject has given explicit Consent to the proposed transfer; or
- The transfer is necessary for the performance of a contract between the Data Subject and Institute of Technology Tallaght, or the implementation of pre-contractual measures taken in response to a request by a Data Subject; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Institute and a Third Party; or
- The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or
- The transfer is required by law; or
- The transfer is necessary to protect the Data Subject's vital interests; or
- The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

The DPO and the Institute's legal advisors must assess whether any of the above exceptions apply prior to any Personal Data transfer and must record the determination in writing.

2.13 Third Parties Relationships

Where a School and Function engages 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, School and Functions must enter into a written contract, or equivalent. This contract or equivalent:

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

School and Functions must ensure that all Third Party relationships are established and maintained.

2.14 Data Subjects Rights

The DPO, supported by the Head of Schools and Functions, shall maintain appropriate processes and procedures to address Data Subjects rights when exercised under GDPR and relevant EU Member State Data Protection requirements. Data Subject information requests are likely to include:

- Right of Access;
- Right to Rectification;
- Right to Erasure (sometimes referred to as the Right to be Forgotten);
- Right to Restriction of Processing;
- Right to Data Portability;
- Right to Object to Direct Marketing;
- Right to Object to Automated Decision Making, including Profiling.

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)
- Provided in a timely manner

School and Functions must notify the DPO immediately when in receipt of a Data Subject information request and must provide the DPO with all necessary support to allow a response in accordance with regulatory timelines.

2.15 Education and Awareness

School and Functions 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. The Institute will maintain employee GDPR training completion records.

2.16 Oversight and Support

In order to ensure the Institute's GDPR requirements compliance, the DPO, supported by the Head of Schools and Functions, will.

- Monitor business line quality control and quality assurance testing results,
- Monitor Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) and required School and Functions compliance reports established in accordance with the operational risk framework, and
- Oversee other appropriate monitoring and testing results.

2.17 Subject Access Request (SAR)

2.17.1 Purpose

The Institute processes certain personal data relevant to the nature of the employment of its employees, students and, where necessary, to protect its legitimate business interests. As such the Institute is the Data Controller for this personal data. GDPR confers certain rights to Data Subjects including the right of access to personal data held by organisations. This policy outlines how Data Subjects may access personal data held by the Institute and how the Institute complies with GDPR with respect to access.

2.17.2 Fees and refusals of subject access requests under GDPR

GDPR abolished the €6.35 subject access request fee under previous data protection legislation. However, the Institute under GDPR 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.
- Refuse to act upon the request.

The Institute 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.

2.17.3 Data Protection Officer (DPO)

The Institute in meeting its data privacy commitments has appointed a Data Protection Officer (DPO) as the point of contact for all data privacy queries that employees and students may have including subject access requests. The contact details of the Data Protection Officer are available on the Institute website.

2.17.4 GDPR Business Processes Personal Data Inventory

The Institute has created a GDPR business processes personal data inventory as part of the GDPR compliance program. This details all business processes that involve the processing of personal data, the basis for doing so, retention periods for this personal data, what the personal data is used for, and whether this personal data is transferred to a third party.

2.17.5 Submission and Processing Procedure for a Subject Access Request (SAR)

Employees and students of the Institute should contact the Data Protection Officer 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 Data Protection Officer for response.

All subject access requests must be made via the Subject Access Request (SAR) form (see Appendix D.) that is available on the Institute website. All subject access requests shall be directed to the Data Protection Officer and all requests shall have an open status until an action by the Data Protection Officer sets a closed status.

The Data Protection Officer upon receipt of the request shall in the following order:

1. Contact the data subject or their representatives confirming receipt of the request along with the date the request was received. In addition, if there is any doubt regarding the identity of the requestor, the Data Protection Officer may request a valid photo ID as additional proof of identity.

2. Determine if the request should be refused under GDPR. If the request is to be refused then the Data Protection Officer shall contact the data subject to inform them of this and shall set the status of the request as closed providing details of the case closure.

3. Determine the effort involved in satisfying the request. If the Data Protection Officer determines that the effort involved means:
    a) The request cannot be satisfied within the 1 month GDPR timeline but can be satisfied with an extension then the Data Protection Officer shall contact the requester and inform them of the need for an extension as well as the reason why an extension is required, and also an approximation of when the request requirements will be met. This contact shall be documented on the open request.
    b) If there is a requirement for the charging of a fee then the Data Protection Officer shall contact the requester and inform them of this need. The requester must then decide whether they are proceeding with the request or whether they wish to terminate the request. This contact shall be documented on the open request and depending on the decision of the requester the DPO shall either close the request or continue to fulfil the request.

4. Once the request is completed then the Data Protection Officer shall contact the requester telling them that the request is available in the format that they requested and that they should call for collection, or if it is an external requestor, that the request will be sent via official correspondence once their identity has been confirmed (see next step).

5. The Data Protection Officer shall verify the identity of the requester by their employee ID card/student ID card (if internal requestor) or official ID documentation (e.g. passport, driver's license) (if external requestor) before the transfer of data is complete.

6. The Data Protection Officer shall close the open request.

2.18 Data Encryption

2.18.1 Purpose

The purpose is to provide guidance on the encryption of (strictly) confidential and/or personal information contained, processed or transmitted within hardware and software resources that are owned and/or operated by the Institute.

2.18.2 Scope

This applies to all Institute staff and students as well as any external parties (e.g. contractors, etc.) with access to information hardware and software resources. It covers (strictly) confidential/personal data at rest (data stored, including that retained on portable devices or removable media), data in transit (transmission of information), and also encryption key standards and management. It also addresses all (remote or on site) connections made to Institute domains (e.g. WiFi, LAN etc.), and all connections made to external sites through the Institute's network.

2.18.3.1 Situations Requiring Encryption

Encryption is necessary in order to protect (strictly) confidential/personal data pertaining to employees, students and other affiliates of the Institute and is required in the following situations (among others):

- Disk encryption for laptop and desktop computers.
- Password encryption/hashing.
- Backup data where the backup media is sent outside of an Institute facility or a facility managed on behalf of the Institute.
- Remote access and VPN communication channels.
- Mobile computing equipment storage media and backups.
- Data communications for externally facing applications transferring (strictly) confidential and/or personal data (as defined under GDPR).
- Web services communication/interactions transferring (strictly) confidential and/or personal data (as defined under GDPR) beyond the Institute's data centre.

2.18.3.2 Data at Rest

Data at rest is data that is saved in persistent storage like disks or tape. Data at rest can reside in the file system or in the data tier as individual data elements. Encrypting data at rest protects sensitive data and meets regulatory compliance requirements.

Depending on its data classification, data at rest may need to be encrypted so it is not readable by any user or application without a valid key.

- For internal data: Encryption not required.
- For confidential data: Encryption required anywhere
- For strictly confidential data: Encryption required anywhere.

Strong key management is required for encrypted data at rest to reduce the risk of unauthorised access to the data. How this policy applies to each device owned and/or operated by the Institute is summarised below:

1) Servers

(Strictly) confidential data stored on shared network servers which are situated in insecure locations (e.g. remote print servers) must be protected by the use of strict access controls and encryption software.

2) Desktop Computers

(Strictly) confidential data at rest on computers owned by the Institute and located within controlled spaces and networks should be protected by encryption with strict access controls that authenticate the identity of those individuals accessing the specific system or data.

Encryption software should be installed in the following:

A. Any desktop computer owed and/or operated by the Institute that is located in an external (third party) facility.
B. Any desktop computer owed and/or operated by the Institute that is located in a public area (e.g. at a reception desk).
C. Any desktop computer owed and/or operated by the Institute that is located in the home of an Institute employee.
D. Any desktop computer owed and/or operated by the Institute that permanently stores (strictly) confidential/personal information or hosts information systems that process such data on the local hard drive, rather than on a secure server.

The method of encryption required for the Institute's desktop computer devices is whole disk encryption.

Note: hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, or are unencrypted, but connect to encrypted USB devices, may be vulnerable to information spillage from the encrypted region into the unencrypted region. Whole disk encryption avoids this problem.

3) Laptops, Tablets, Mobile Phones and other Smart Devices

(Strictly) confidential data should not be stored on these portable devices, as loss or theft of these devices can result in unauthorised data exposure and thus constitute a data breach. If (strictly) confidential information must be stored on such devices, whole disk encryption reduces the risk of unauthorised data access should the theft or loss of the device occur.

Mobile computer devices and smart devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all (strictly) confidential and restricted information stored on the device. All portable devices must have up to date antivirus software and password protection enabled, in addition to data encryption.

All users should obtain permission from the Data Protection Officer prior to storing (strictly) confidential information on portable devices, and under no circumstances should these devices be used for the long term storage of such information.

Portable or removable media that contain (strictly) confidential data must be in the possession of the authorised user at all times (e.g., must not be checked as luggage). Users of portable computing devices containing (strictly) confidential data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. This can be done by:

- Maintaining a copy of each encryption key in usage on a secure server managed by the Institute, including procedures specified by the DPO.
- Using encryption that allows an authorised system administrator access to the data in the event that an encryption key is forgotten.

4) Removable Storage Devices

All (strictly) confidential and restricted information stored on removable storage devices (e.g. USB memory sticks, CD-ROM's, floppy disks, backup tapes/drives and DVD's) must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use. The following criteria also apply:

- The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all (strictly) confidential and restricted information stored on the removal storage device.
- Removable storage devices except those used for backup purposes must not be used for the long-term storage of (strictly) confidential and restricted information.
- (Strictly) confidential data should be transferred from removable storage devices to a secure Institute server at the earliest opportunity, and subsequently deleted from the removable storage device.
- (Strictly) confidential and restricted information stored on the encrypted removable storage device must not be transferred to any internal (except a secure network server) or external system in an unencrypted form.
- Removable storage devices containing (strictly) confidential information must be transported using a secure manner. Devices sent offsite for storage by a third party must have an accompanying chain of custody forms for possession tracking purposes.
- An annual inventory of all encrypted removable storage devices should be carried out, and should also determine the effectiveness of the encryption method/software in use.
- Users of portable computing devices containing (strictly) confidential data must acknowledge how they will ensure that data is encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten. See the methods for achieving this outlined in Section 3 above.

2.18.3.3 Data Transmission

All (strictly) confidential or restricted information transmitted through email to an email address outside of the Institute's domain must be encrypted. The transfer of such information must be authorised by the Head of School/Function and/or the DPO. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

Where (strictly) confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channels (for example: Secure FTP, TLS, VPN etc). The transfer must be authorised by the Head of School/Function and/or the DPO. The authorisation must be issued in advance of the first instance and will apply thereafter if necessary.

All (strictly) confidential and restricted information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy) or better. All new wireless networks installations must be encrypted using WPA (Wi-Fi Protected Access) or better.

Wireless (Wi-Fi) transmissions that are used to access portable computing devices or internal networks must be encrypted using standard. Encryption is required when users access data remotely from a shared network, including connections from a Bluetooth device to a PDA or cell phone.

If a secure server is used to enable the encrypted transfer of documents and data over the Internet using file transfer programs, each authorized user must have a logon ID and password with a designated directory. Anonymous users/access to an Institute FTP site is not permitted.
All accounts and keys must be managed from within network. All transactions and transfers must be logged, and reviewed for prohibited activity.

2.18.3.4 Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

The individual with responsibility for encryption key management (e.g. Head of IT, etc.) will verify backup storage for Key passwords, files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.

Separation of duties and two person control prevent the generation of a new encryption key by a single individual. Regular (e.g. quarterly) reviews will be conducted to verify the identity of all subjects responsible for key management functions and the generation of new encryption keys. Training should be provided to all relevant personnel on key management requirements and procedures.

Keys must be randomly chosen from the entire key space, using hardware-based randomization. Key-encrypting keys are separate from data keys. No data ever appears in clear text that was

encrypted using a key-encrypting key, e.g., a key-encrypting-key is used to encrypt other keys, securing them from disclosure. The following points are also addressed by encryption key management policy:

- Encryption keys that support a production environment must be bound to the Institute.
- All encryption keys and key management procedures must have an identified owner to ensure accountability to an individual identity within the Institute.
- Cryptographic modules that are used for storing keys must be backed up using approved encryption strength technology (e.g. accredited to FIPS 140-2 Level 2).
- Private keys must be kept confidential.
- Keys in transit and storage must be encrypted.
- Keys must be destroyed at the end of their crypto period.
- Key-generating equipment is kept physically and logically secure from construction through receipt, installation, operation, and removal from service.

2.19 Data Anonymisation/Pseudonymisation

2.19.1 Purpose and Scope

The purpose is to provide guidance on the anonymisation and/or pseudonymisation of (strictly) confidential and/or personal information contained, processed or transmitted within hardware and software resources that are owned and/or operated by the Institute. It applies to all Institute students, staff, and any external parties (e.g. contractors, etc.) with access to information hardware and software resources. It covers all (strictly) confidential/personal data at rest (data stored, including that retained on portable devices or removable media) and in transit (transmission of information).

2.19.2 Anonymisation and Pseudonymisation

Anonymisation and Pseudonymisation are two methods of processing (strictly) confidential data, in such a manner that the confidential data in question cannot be traced back to the individual 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.

2.19.2.1 Anonymisation

When anonymising data, the Institute must be certain that all information is assessed, and the risk of re-identification is evaluated. This entails examining whether other information is available that, in combination, is likely to facilitate re-identification of the anonymised information. Re-identification is most likely to occur where circumstances described by the combined information are unusual or the population sizes in question are very small.

A "motivated intruder" test should be carried out as a method to check whether the information has been anonymised effectively. This test checks whether a competent individual with the aim of de-anonymising the data could do so successfully.

This test involves discovering whether easily available online/physical information exists that can be used in combination "a jigsaw attack" to re-identify the data subjects to whom the anonymised data pertains. Such resources could include social media, library archives, press archives, electoral register etc.

Re-identification of a data subject would lead to the unauthorised disclosure of (strictly) confidential information and thus constitute a data breach. Any such event should be reported as soon as possible to the DPO.

Members of staff, students and external affiliates of the Institute should only have access to the level of identifiable information that is necessary for them to complete their assigned activity. However, through effective anonymisation, these activity owners are able to make use of anonymised data for a range of secondary purposes.

Effective anonymisation is achievable via a range of techniques, depending on the nature of the dataset in question and how suitable the chosen technique is. Samples of techniques include:

- Removing personal identifier(s).
- Using identifier ranges (e.g. age range instead of age, partial postcode, age at time of activity event instead of date of birth, output area instead of full address etc.)
- Aggregation – information is only viewed as totals rather than individual data values.
- Randomisation – informational "noise" injected into the dataset to prevent data identification (e.g. the age/height of the individual being increased or decreased by a small amount to avoid identification).

De-identified or anonymised information that goes down to the level of the individual should still be stored and used within a secure environment that has restricted access privileges.

2.19.2.2 Pseudonymisation

Pseudonymisation is the process of distinguishing identities. The aim of such a process (vs anonymisation) is to be able to collect additional data relating to the same individual without having to know the identity.

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individuals across different datasets and over time. This allows datasets and other information to be

linked in ways that would not be possible if person identifiable information was removed completely.

This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index.

To effectively pseudonymise information, the following actions must be taken:

- Each field of person identifiable information must have a unique pseudonym;

- Pseudonyms to be used in place of identifiable information (e.g. date of birth etc.) and similar fields must be of the same length and formatted on output to ensure readability. For example, in order to replace date of birth in existing record formats, the output pseudonym should generally be of the same field length, but not of the same characters, to avoid confusion with real person identifiable information.

- Generalisation – Diluting information so that identification of individuals is impossible (e.g. instead of date of birth, use year of birth etc.).

- Consideration needs to be given to the impact on existing systems, both in terms of the maintenance of internal values and the formatting of reports;

- Where used, pseudonyms for external use must give different pseudonym values in order that internal pseudonyms are not compromised;

- The secondary use output must, where pseudonyms are used, only display the pseudonymised data items that are required;

- Pseudonymised information should have the same security as person identifiable information.

3. Training and Awareness

The Institute is committed to the provision of data protection training on a mandatory basis 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 personal data in the course of their everyday business.

To achieve this the Institute will support the development, rollout and communication of Data Protection training and an awareness program across the Institute. This program will ensure that staff are regularly reminded of policies throughout the year and not simply when a policy is updated. In addition refresher sessions, briefings and reminders will occur at regular intervals.

For on-line 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 personal data' and know how to handle such data;
- Not jeopardise individuals' rights or risk a contravention of the Act;
- Contact their Head of School / Function or DPO if in any doubt

Appendix A – Data Processing Register Example Template

Personal Data Process-ing Activity	Categories of personal data and data subjects	Elements of personal data included within each data category	Source of the personal data	Purposes for which personal data is processed	Legal basis for each processing purpose (non-special categories of personal data)	Special categories of personal data	Legal basis for processing special categories of personal data	Retention period	Transfers to third parties and third countries	Transfers to third countries and appropriate safeguards	Technical and Org Controls	Action required to be GDPR compliant?
Identify the personal data processing activity being assessed e.g. Student enrollment	*List the categories of data subjects and personal data collected and retained e.g. current employee data; retired employee data; customer data (sales information); marketing database; CCTV footage.*	*List each type of personal data included within each category of personal data e.g. name, address, banking details, purchasing history, online browsing history, video and images.*	*List the source(s) of the personal data e.g. collected directly from individuals; from third parties (if third party identify the data controller as this information will be necessary to meet obligations under Article 14).*	*Within each category of personal data list the purposes for the data is collected and retained e.g. marketing, service enhancement, research, product development, systems integrity, HR matters, advertising.*	*For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, contract, legal obligation (Article 6).*	*If special categories of personal data are collected and retained, set out details of the nature of the data e.g. health, geneticx, biometric data.*	*List the legal basis on which special categories of personal data are collected and retained e.g. explicit consent, legislative basis (Article 9).*	*For each category of personal data, list the period for which the data will be retained e.g. one month? one year?* *As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.*	*List third parties in receipt of personal data e.g. Banks*	*List transfers of data to territories outside of the European Economic Area and safeguards in place (e.g. EU Model Clause)*	*Provide a general statement of the technical and organisational security measures taken specifically for the processing activity.* *Technical and organisational security measures taken at business level do not need to be mentioned specifically. For these simply list 'Standard measures.'*	*Identify actions that are required to ensure all personal data processing operations are GDPR compliant e.g. this may include deleting data where there is no further purpose for retention.*

Source: *Office of the Data Protection Commissioner GDPR Checklist (columns in orange added by PwC)*

Appendix B – Privacy Notice Requirements

Have you reviewed your privacy notices yet? Do they include the following?

Identity and contact details of the controller	☐
Contact details of the Data Protection Officer	☐
Details of the purposes and legal basis for the processing of personal information	☐
Details of the legitimate interests the processing is based on (if applicable)	☐
Recipients of the personal data	☐
Details of transfers to third countries and the safeguards that are in place (if applicable)	☐
Details of how the data subject can obtain a copy of data transferred to third countries and how to obtain a copy of this data (if applicable)	☐
Retention period or the criteria used to determine a retention period	☐
Details of the data subject's right of access to and deletion/rectification of personal data, their right to objection to processing and to portability	☐
Details of the right to withdraw consent (if applicable)	☐
The data subject's right to lodge a complaint with the supervisory authority	☐
Details of the consequences when a data subject neglects to provide personal data when they are obliged to do so	☐
Details of automated decision making (if applicable) including logic used and consequences to the data subject	☐

Appendix C - Data Protection Impact Assessment Exemplar

Procedures

Background:
Data Protection Impact Assessments ('DPIAs') can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect Institute of Technology Tallaght. DPIAs are mandatory for any new high risk processing projects.

When to use a DPIA:
Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons." This is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law. The DPIA should be carried out prior to the processing of data by Institute of Technology Tallaght.

Who must carry out the DPIA:
It is the responsibility of the project team to ensure that a DPIA is carried out for any new high risk processing projects.

DPIA Process:

1. **Identifying whether a DPIA is required:**
   Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified

2. **Describe the information flows:**
   Describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

3. **Identify data protection and related risks**
   Identify the key privacy risks and the associated compliance and corporate risks.

4. **Identifying data protection solutions to reduce or eliminate the risks**
   Describe the actions you could take to reduce the risks, and any future steps which would be necessary.
5. **Signing off on the outcomes of the DPIA**
   Ensure appropriate sign off of outcomes is formally documented and retained.

6. **Integrating data protection solutions into the project**
   Ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld.

Template

1. Identifying whether a DPIA is required Please answer the below screening questions	
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?	
Is a Data Protection Impact Assessment required to be performed? (If answering 'yes' to any of the above performing a DPIA is advisable)	

2. Describe the information flows	
Date of Assessment:	
Assessment performed by:	
Function/Department:	
Process Name:	
Description of the envisaged processing operations: (Including collection, deletion and use)	
Purposes of the processing:	
Legal basis for processing:	
Necessity of the processing (Justification)	
Proportionality of the processing (Estimated number of Data Subjects Affected)	
Individuals consulted during the performance of DPIA (Include internal and external consultations held)	

3. Identify data protection and related risks			**4. Identifying data protection solutions to reduce or eliminate the risks**				
No.	Privacy Issue	Risk	Existing Controls Identified	Risk Rating L x I	Additional Controls/ Actions Required	Action Owner	Deadline Date
1							

5. Signing off on the outcomes of the DPIA	
DPIA Assessment result: (Pass- risk eliminated, avoided or accepted; Fail- risk avoided)	
Approved by:	
6. Integrating data protection solutions into the project	
Next steps/Actions	

Guidance

Example Risks to Individuals:

- Inappropriate disclosure of personal data internally within the organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- 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.

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.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. 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 the organisation may also be liable for non-material damage.

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:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- 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 portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with the organisation.
- If using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements 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.

Risk Assessment Guidance:

Likelihood/Potential for an Incident to occur	Impact/Outcome of Incident	Risk Level Calculation L X I	Guideline Action Timetable
1 - Rare: No history of event occurring over period of years. This event may occur but in exceptional circumstances.	**1.** Minor compromise of privacy (e.g. un-sensitive personal data such as helpdesk ticket compromised)	1 – 2 Acceptable	No Action
2 - Unlikely: The event would be expected to occur annually	**2.** Minor data breach (e.g. inappropriate contact of data subject via email)	3 – 5 Low	Prioritise after medium risk actions complete
3 - Possible: This could occur monthly, as such it has a reasonable chance of occurring.	**3.** Moderate data breach (Sensitive data e.g. payroll compromised)	6 – 10 Medium	Prioritise after high risk actions complete
4 - Likely: Expected to occur at least weekly, the event will occur in most situations	**4.** Significant data breach (Financial loss, severe stress for a data subject or data subjects	11 – 15 High	Prioritise Action as soon as Practical
5 - Certain: Expected to occur almost daily, it is more likely to occur than not.	**5.** Major data breach (Risk of severe financial loss to a large number of data subjects)	16 – 25 Very High	Action Urgent

Appendix D – Subject Access Request (SAR) Form

Please describe the information you are looking for, including dates and locations where

Subject Access Request Form

Under the General Data Protection Regulation (GDPR) it is you right to request a copy of any personal data that we hold on you. Please note that this form is to aid the Subject Access Request process.Further information on the Subject Access Request process can be found at [Link to Info doc]

Name (Last, first, middle initial) Date

PPS Number

Address

Primary phone number | Other phone number Email address

Name Date

Signature Date

For Employee Use Only

Received By:

Name Date

Please scan this form and send to XXXXXXXXXXXXXXX