Data Protection Policy

Section 1: Data Protection Policy

1.1 Background

The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 confer rights on individuals and govern the processing of all personal data in all organisations including DIT. The purpose of the Data Protection (DP) Acts is to safeguard the privacy rights of individuals regarding the processing of their personal data by those who control such data.

As part of its mission DIT is required to collect, use and keep personal data (information) about its staff, students and other individuals who come in contact with the Institute in accordance with the functions outlined in those DP Acts,.

The purposes of processing this data by DIT include the organisation and administration of courses, research activities, the recruitment and payment of staff, compliance with statutory obligations and compliance with legal obligations to funding bodies and government, etc. To comply with the relevant legislation, data about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully by DIT. Under regulations introduced by the Minister for Justice, Equality and Law Reform on 1st October 2007, DIT is no longer required to register with the Office of the Data Protection Commissioner as a Data Controller and, therefore, does not appear on the Public Register. DIT is, however, still obliged to comply with the general provisions of the DP Acts. All documents created and received by the Dublin Institute of Technology (DIT) in the course of its official business (including teaching, research and administration) as laid out in the Dublin Institute of Technology Acts, 1992 and 1994 and the Institutes of Technology Act, 2006, constitute the official records of DIT.

Records Management is the application of systematic control over information which is required in the administration and operation of DIT's activities. The information that DIT records contain serves as evidence of functions executed and activities performed and comprise a valuable source of knowledge as to how and why decisions were taken. Records created or received by DIT staff in the course of their duties on behalf of the DIT, can be in a variety of physical forms including: paper documents including both written and printed matter, books, drawings, electronic data on any media, photographs, or anything on which information is recorded or stored by graphic, electronic or mechanical means, or copies thereof received by an academic or administrative office of DIT in connection with the transaction of DIT business and retained by such office as evidence of the activities of DIT or because of the information contained therein.

In addition to DP legislation, it is worth noting that Freedom of Information (FOI) has since its introduction in 1998 made a major contribution to facilitating access by citizens to official information. It has contributed to a shift towards greater openness and transparency in the conduct of official activities and in Ireland's administrative and political culture. FOI requests are made and responses are sought in various formats and there are legal complexities in the interaction with other legislation such as the Data Protection Acts and other access to information regimes. It is important that a strong framework must be in place within each public body to support the effective implementation of the FOI Act 2014. The structures put in place in each public body are pivotal to the effective performance of the public body in relation to delivering on their commitment to quality in meeting their obligations under FOI as well as minimising the administrative burden of FOI. The details of these are contained in a separate Freedom of Information Policy of DIT.

This Data Protection Policy addresses statutory Data Protection and Records Management requirements of DIT and refers to FOI and Information Services (IS) IT Security Policies as necessary.

1.2 Purpose of this Policy

The purpose of this policy is a statement of DIT's commitment to protect the rights and privacy of individuals in accordance with the DP Acts and to outline principles for the classification, handling and administration of the data of DIT in that regard. This policy applies to all areas and locations of DIT and includes all departments, offices, units, research centres and areas of work which form part of the institutional structure. This policy is equally applicable to records created and preserved in both paper and electronic format.

1.3 Definitions used in the Data Protection Acts

The following definitions have been adapted from Section 1 of the DP Acts and are used in this Policy (See www.dataprotection.ie):

- ***Data*** means both automated and manual data.
  The word "data" is often used interchangeably with the word "record" or "information" in common usage and includes coded representation of quantities, objects and actions processed into a form that has meaning and value to the recipient to support an action or decision.

    - Automated data means any information on computer, or information recorded with the intention that it be processed by computer.
    - Manual data means information that is recorded as part of a relevant filing system or with the intention that the data form part of a system.

- ***Data Controller*** means a body that, either alone or with others, controls the contents and use of personal data.

- ***Data Processor*** means a person who processes personal data on behalf of a Data Controller but does not include an employee of a Data Controller who processes such data in the course of his employment.

- ***Data Subject*** means an individual who is the subject of personal data.

- ***Personal Data*** means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.

- ***Processing*** means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

    - Obtaining, recording or keeping the information, or
    - Collecting, recording organising, storing, altering or adapting the information or data,
    - Retrieving, consulting or using the information or data
    - Disclosing the information or data by transmitting, disseminating or otherwise making them available, or
    - Aligning, combining, blocking, erasing or destroying the information or data.

- ***Relevant Filing System*** means any set of information relating to individuals to the extent that, while not computerised, is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

- ***Sensitive Personal Data*** means personal data which relate to specific categories defined as:

    - The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
    - Trade union membership
    - The physical or mental health or condition or sexual life of the data subject
    - The commission or alleged commission of any offence by the data subject, or
    - Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

It is also worth noting that Personal data of a financial nature is viewed similarly to Sensitive Personal Data by the Data Protection Commissioner and means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

1.4 Data Protection Principles

As a Data Controller, DIT must comply with the 8 Data Protection Principles or Rules which are set out in the DP Acts and administer its responsibilities under that legislation in accordance with these stated principles as follows:

(i) *Obtain and process information fairly*

DIT will obtain and process personal data fairly and in accordance with the fulfilment of its functions as set out in the DIT Acts, 1992 and 1994 and the IOT Act, 2006.

(ii) *Keep data only for one or more specified, explicit and lawful purposes*

DIT will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

(iii) *Use and disclose data only in ways compatible with these purposes*

DIT will only disclose personal data that are necessary for the purpose(s) or compatible with the purpose(s) for which it collects and keeps the data.

(iv) *Keep data safe and secure*

DIT will take appropriate security measures against unauthorised access to, or alteration, disclosure, destruction or unlawful processing of the data and against their accidental loss or destruction.

(v) *Keep data accurate, complete and, where necessary, up-to-date*

DIT will have procedures that are adequate to ensure high levels of data accuracy and appropriate procedures to keep data up-to-date.

(vi) *Ensure that data are adequate, relevant and not excessive*

Personal data held by DIT will be adequate, relevant and not excessive in relation to the purpose(s) for which it is collected and kept.

(vii) *Retain data for no longer than is necessary for the purpose or purposes*

DIT has a policy on retention periods for personal data which is contained in the Records Management Principles in Section 1.8 below.

(viii) *Give a copy of his/her personal data to that individual, on request, and correct the data or, in certain cases as defined in the DP Acts, block or erase the data where that individual so requests*

DIT will have procedures in place for Data Protection Subject Access Requests to ensure that data subjects can exercise their rights under the Data Protection legislation.

Further Information in relation to **DIT Data Protection Procedures and Guidelines** is available in Section 2.

1.5 Data Classification and Data Handling

The Institute as a public organisation subject to FOI, has the following four classifications of Data:

- Private data,
- Public data,
- Sensitive Personal data and
- Personal data.

Each category of data requires a different form of security or protection based on potential breach of legislation or the strategic impact to the Institute if the security if that data was compromised.

The Institute in addition to the classifications above has a data handling policy that sets out the manner in which the various types or classes of data set out in the data classification should be managed across the data flow lifecycle i.e. from collection, storage, transmission, processing to destruction.

Further Information is available in Section 3.

1.6 Personal Data Security Breach Management

A Personal Data security breach ("data breach" in short) occurs when Personal Data is made available to one or more third parties without the consent of the data subject. Data breaches may occur in a variety of contexts, e.g.:

- Loss or theft of data (e.g. on a memory stick, laptop or paper records)
- Inappropriate access controls (e.g. using unsecure passwords)
- Equipment failure

- Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
- Disclosing confidential data to unauthorised individuals
- Human error (e.g. emails being 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).

If you consider that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing **Personal Data Security Breach Report Form** in Section 4.2. Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

It is much better to report a data protection breach straight away than to "cover it up" and risk negative consequences down the line. A data protection breach is not a disciplinary issue, and once the breach has been reported the Information Governance Officer will handle things from there.

There is a requirement that all incidents in which personal data has been put at risk must be reported to the Data Protection Commissioner within 2 days of DIT becoming aware of the incident.

Subsequent to each data security breach a log will also be maintained by the Information Governance Officer of the agreed steps arising from each incident and this will be presented by way of an overall annual report to the President or his nominated Committee.

Further Information is available in Section 4.1.

1.7 Data Protection Subject Access Requests

Under the Data Protection Acts, 1988 and 2003, an individual may receive a copy of any personal data relating to them which is held by DIT (a Subject Access Request). Anyone who wishes to make a request for access to their personal data can do so by completing the **Data Protection Subject Access Request Form** in Section 5.2.

The Requestor is encouraged to give as much information as possible about the data they wish to access, they must include proof of identity (e.g. a copy of their passport, drivers licence or staff/student ID card) and a fee of €6.35 is payable with the application. A decision in relation to requests made under Section 4 of the Data Protection Acts (access to personal information) will be made within 40 days of receipt of the request. If the individual is not satisfied with the response to their request, they may contact the Data Protection Commissioner, who will investigate the matter for them.

Requests can also be made by an individual to:

- Establish whether DIT holds Personal Data relating to them or
- To cease processing Personal Data on the grounds that it would cause unwarranted damage or distress to the individual Data Subject or
- To correct, block or erase their Personal Data.

Further Information is available in Section 5.

1.8 Records Management Principles

Records Management is the application of controls to the creation, maintenance, use and disposal of all formats of records which includes correspondence and forms, records classification, files, identification of staff member responsible for the record, retention scheduling, disaster planning, vital records protection, record conversion programmes, archival preservation activities and appropriate destruction of records.

A **Records Retention Schedule**, as detailed in Section 6.5, is a control document that lists the main records that DIT creates, receives or maintains in the course of its official business and indicates the length of time that records shall be retained for before final disposition and the method of disposition.

Schedules are based on a determination of legal retention requirements as defined in relevant statutes and regulations, financial requirements, administrative requirements and operational requirements. While the Retention Schedules prescribe the minimum period that DIT records must be retained, these may be retained for a longer period of time if it is deemed necessary by the Head of Function for operational or administrative requirements.

The final disposition (either destruction or transfer to storage) of records is carried out following review of the DIT Retention Schedules, as detailed in the **Disposition of Records / Data Register Form** in Section 6.6, after which time the records / data are either destroyed or transferred to DIT storage or Archives. The potential historical value of records is also a consideration.

The Records Retention Schedule applies to both electronic and paper records held by DIT and in the absence of any electronic records management systems, staff should be encouraged to employ good housekeeping practices in the management of electronic documents, i.e. employ a naming convention, have a back-up schedule, delete regularly (especially e-mails), use passwords as appropriate, produce paper copies if required to maintain the integrity of manual files, etc.

Effective electronic records management requires consideration of the appropriate electronic software in the context of an overall records management programme. Electronic records should have the same retention schedules as their paper counterparts. In the case of electronic records, the department which created or maintains these records must formally agree back-up and recovery procedures with the Information Services Department. This is to ensure that there is no ambiguity as to which department is responsible for records in the event of hardware failure or accidental deletion of records.

All records, both paper and electronic created or received by DIT staff in the course of their duties on behalf of DIT, are the property of DIT and subject to its overall control.

Further Information is available in Section 6.

1.9 Roles and Responsibilities

DIT through the President and the Senior Leadership Team has overall responsibility for ensuring compliance with the Data Protection legislation and this Policy. However, all employees (where they are employed) or students (in the course of their studies) of the Institute who collect and / or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation and this Policy.

This Policy also applies to individuals who are not directly employed by the Institute, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the Institute as well as Institute clubs and societies.

Failure to comply with this policy may lead to disciplinary action, up to and including dismissal in the case of staff or expulsion in the case of students, being taken in accordance with the Institute'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.

1.9.1 Role of the Senior Leadership Team

The Senior Leadership Team is responsible for the internal control of DIT, 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. The SLT is responsible for:

- reviewing and approving this Policy and any updates to it as recommended by the Office of the Institute Secretary;
- ensuring ongoing compliance with the Data Protection Acts in their respective areas of responsibility;
- As part of the Institute's Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the Data Protection Acts.

1.9.2 Role of the Information Governance Officer

The Institute has appointed an Information Governance Officer (contact details below) in the Office of the Institute Secretary who will assist the Institute and its staff with compliance with the DP Acts and the FOI Act.

The Information Governance Officer is the Senior Officer within the Institute responsible for statutory compliance with the Data Protection Acts and is also responsible for:

- ensuring that this Policy is reviewed and approved by the SLT as appropriate;
- ensuring that appropriate policies and procedures are in place to support this Policy;
- ensuring that any data security breaches are properly dealt with and liaising with the Office of the Data Protection Commissioner where necessary/appropriate;
- processing and responding to formal Data Protection Subject Access Requests while liaising with relevant Decision Makers in Institute departments/offices regarding such requests;
- initiating regular reviews of data protection policies and procedures and ensuring documentation is updated as appropriate;
- organising targeted training and briefing sessions for Institute staff as required;
- providing advice and guidance to Institute staff on data protection matters;
- maintaining a centrally-held register of the categories of personal data held by Institute;
- Maintaining a list of nominated contact persons with responsibility for coordinating data protection matters within their own areas.

1.9.3 Role of Head of School / Function

It is the responsibility of each Director to designate each Head of Function as the owner of records in their area. Where records are used by more than one area, it is the responsibility of each area to ensure that the ownership of the record is agreed and established.

Each Head of School / Function must ensure that the Information Governance Officer is informed of any changes in uses of personal data that might affect DIT's compliance with the DP Acts. It is the responsibility of the Head of School / Function to ensure that appropriate security measures are observed for maintaining records containing personal or other confidential information.

Every School and Function within the Institute which processes personal data is required to nominate a suitable member of staff to be responsible for coordinating Data Protection compliance matters within their respective area, such matters to include:

- Being a point of contact for the Information Governance Officer regarding Data Protection;
- Bringing relevant Data Protection / IT data security matters to the attention of relevant staff in his/her area;
- Participating in training in data protection / IT data security where appropriate.

1.9.4 Role of Data Protection Commissioner

The Data Protection Commissioner oversees national compliance with the terms of the legislation. The Office of the Data Protection Commissioner (ODPC) has a wide range of enforcement powers, including investigation of Institute records and record-keeping practices. Summary proceedings for an offence under the DP Acts may be brought and prosecuted by the ODPC.

Under Section 31 of the DP Acts, the maximum fine on summary conviction of such an offence is set at €3,000. On conviction on indictment, the maximum penalty is a fine of €100,000. A Data Controller found guilty of an offence can, in addition to a fine, be also ordered to delete data. Extensive information is available from the Data Protection Commissioner at www.dataprotection.ie.

1.10 Training and Awareness

The Institute is committed to the provision of data protection training on a mandatory basis as well as necessary in addition to on an opt-in basis to ensure all individuals are aware of their respective obligations under Data Protection legislation. 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 DIT. 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 Data Protection set out in this Policy;
- Read and understand this policy document;

- 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 Information Governance Officer if in any doubt.

1.11 Monitoring and Auditing

The Institute is committed to ongoing review, monitoring and periodic auditing of the control processes for ongoing compliance with Data Protection policies, procedures and guidelines.

The Institute as part of this will review and audit existing controls over personal information by completing and updating detailed current state assessments of data protection controls and the development of a central register of personal data held by DIT (in both paper and electronic forms).

The Institute as part of this review will also complete and update detailed data flow lifecycles with personal data inventories which will classify the data as either personal data or sensitive personal data and categorise the data by functional area and identify a data owner for each category.

Periodic spot checks on compliance with Data Protection policies, procedures and guidelines will be conducted by the Information Governance Officer with the input and support of IS where required.

1.12 Status of this Policy

This Policy has been approved by the Institute’s Senior Leadership Team and Governing Body and applies to all staff and students of the Institute.

If you have any queries or require clarification on any aspect of Data Protection, please contact:

The Information Governance Officer
Office of the Institute Secretary
Dublin Institute of Technology
143 -149 Lower Rathmines Road
Dublin 6
D06 H328

Email: foi@dit.ie
Tel: 01-4027519

Any member of staff or student of the Institute who considers that the Policy has not been followed in respect of Personal Data about themselves should raise the matter with their Head of School / Function or the Information Governance Officer in the first instance.

1.13 Review of this Policy

This Policy will be reviewed annually in light of any legislative or other relevant indicators.

DIT Data Protection Policy Review Record

Approved by	**Approved by the Senior Leadership Team on 07/07/2016**
Next Review Date	**June 2017**
Last Review Date	June 2011
Area of Activity	Information Governance: Data Protection
Policy Author	Information Governance Officer, Office of the Institute Secretary

Section 2: Data Protection Procedures and Guidelines

2.1 Purpose of the Data Protection Procedures and Guidelines

The purpose of these procedures and guidelines is to assist staff and students of DIT in understanding and complying with DIT's Data Protection Policy, which affirms its commitment to protect the privacy rights of individuals in accordance with the legislation. They Procedures and Guidelines set out the areas of work in which Data Protection issues arise (see Section 3 below) and outline best practice in dealing with these issues. These guidelines should be read in conjunction with the current **Information Services (IS) IT Security** related Policies, Procedures and Guidelines.

2.2 Areas in DIT subject to Data Protection

The following is a non-exhaustive list of the systems in DIT, both manual and electronic, where the DP Acts will apply:

- Student and graduate records
- Personnel records
- Administration records
- Library records
- Research data where personal data is held (including files kept by individual staff members and/or students)
- Records of college societies and clubs
- Publishing and editing records.

2.3 Rules of Data Protection

There are eight principles or rules of Data Protection, which govern the processing of personal data. When processing personal data the following procedures apply:

1. *Obtain and process the data fairly;*
2. *Keep the data only for one or more specified, explicit and lawful purposes;*
3. *Use and disclose only in ways compatible with the purposes for which data were initially given;*
4. *Keep data safe and secure;*
5. *Keep data accurate, complete and, where necessary, up-to-date;*
6. *Ensure that data are adequate, relevant and not excessive in relation to purpose for which they were collected;*
7. *Retain data for no longer than is necessary for the specified purpose or purposes;*
8. *Provide a copy of his/her personal data to a data subject, on request, and correct the data or, in certain cases as defined in the DP Acts, block or erase the data where that individual so requests.*

In addition, there are special conditions that must be met before personal data may be transferred to a country outside the European Economic Area (membership composed of the EU member states, Iceland, Liechtenstein and Norway) if that country does not have an EU-approved Data Protection law. Specific provisions are in place concerning personal data transfers to the United States of America.

The above rules apply to all computer held personal data and to all manual personal data created from 1 July 2003. From 24th October 2007, manual personal data created before 1 July 2003 is also subject to the above rules.

2.4 Application of the Rules of Data Protection

In order to ensure the Institute's compliance with these rules, the following procedures must be observed by staff at all times:

RULES NOS. 1, 2 AND 6

Obtaining and processing all personal data fairly

Personal data is obtained fairly if the data subject is aware of the purpose for which DIT is collecting the data at the point of collection, of the categories of person/organisation to whom the data may be disclosed, of non-obligatory or optional answers in forms, of the right of access to the data and of the right of rectification of the data.

- Obtain personal data only when there is a clear purpose for so doing, obtain only whatever personal data are necessary for fulfilling that purpose and ensure data are used only for that purpose.
- It follows that use of DIT data processing facilities in capturing and storing personal data for non-DIT purposes must not take place.
- Inform data subjects of what personal information is held by DIT, what it will be used for and to whom it may be disclosed.
- Obtain explicit consent in writing for processing sensitive data and retain a copy of that consent. Consent cannot be inferred from non-response in the case of sensitive personal data.

RULE NO. 3

Disclosing personal data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of sensitive personal data, the disclosure of which would require explicit consent.

- Except where there is a statutory obligation to comply with a request for personal data, or where a data subject has already been made aware of disclosures, do not disclose to any third party any personal data without the consent of the data subject.

- Verbal consent to disclosure of personal data to the data subject may be obtained by telephone in the case of non-sensitive personal data, but must include asking the data subject to confirm facts that should be known only to them, such as date of birth, student number, etc. The date and time of the giving of the verbal consent should be recorded in writing.

- Verbal consent to disclosure of personal data to a third party is not permitted unless there is a statutory obligation to disclose, or the information is released, to the Gardaí for example, for the prevention of crime and if informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject (see below for permitted disclosures under the DP Acts).

- Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions. Be satisfied of the need to disclose.

- Personal data should not be disclosed outside of the European Economic Area unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

Permitted disclosures of personal data

The DP Acts provide for disclosures, where data are:

- Authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Siochana not below the rank of chief superintendent or an officer of Permanent Defence Forces holding an army rank not below that of colonel);
- Required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or a health board;
- Required to protect the international relations of the State;
- Required urgently to prevent injury or damage to health or serious loss of or damage to property;
- Required by law or a court order;
- Required for legal advice or legal proceedings;
- Disclosed to the data subject or to a person acting on his/her behalf;
- Disclosed at the request or with the consent of the data subject or a person acting on his/her behalf.

RULE NO. 4

Securing personal data

DIT must protect personal data from unauthorised access when in use and in storage and must be protected from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, back-ups, etc.
- Screens, printouts, documents and files showing personal data should not be visible to unauthorised persons.
- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired.
- When upgrading or changing PC, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops and PCs containing personal data are used outside the Institute.
- Health and social work personal data can only be disclosed following consultation with the relevant professional.
- The Institute, on disclosing personal data to a Data Processor, should do so only under a written contract specifying the security rules to be followed.

RULE NO. 5

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and, where necessary, kept up-to-date. Review and audit procedures should be in place to monitor that this is being achieved.

Please refer to section below on 'Responsibilities of data subjects', and particularly the requirement that data subjects should inform DIT of errors in or changes to data. While DIT cannot be held responsible for errors unless previously informed, once informed, it is imperative that the data are amended accordingly.

RULE NO. 7

Retention of personal data

Data should not be kept for longer than is necessary for the purpose for which they were collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose. Personal information should only be held for periods specified in DIT's Records Retention Schedules.

Disposal of personal data

Personal data should be disposed of when they are no longer needed for the effective functioning of DIT. The method of disposal should be appropriate to the sensitivity of the data. Shredding or incineration is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data. Particular care should be taken when PCs are transferred from one person to another or outside DIT or are being disposed of.

RULE NO. 8

Rights of data subjects

Right of access

The DP Acts provide for the right of access by the data subject to his or her personal information.

Data subjects must be made aware of how to gain access to their personal data. A data subject is entitled to be made aware of his or her right of access and to the means by which to access the data. A data subject is entitled to the following on written application within forty days, or sixty in the case of examination data:

- A copy of his or her personal data;
- The purpose of processing the data;
- The persons to whom the Institute discloses the data;
- An explanation of the logic used in any automated decision-making;
- A copy of recorded opinions about him or her, unless given in confidence.

A maximum fee of €6.35 may be charged.

Restriction of rights of access

The right of access is restricted where the data are:

- Required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- Subject to legal professional privilege;
- Kept only for statistical or research purposes and the results are not made available in a way that identifies data subjects;
- Back-up data.

Provision of access to third parties

A data subject is entitled to access his or her own personal data only. The personal information of a data subject, including confirmation of attendance at DIT or contact details, must not be disclosed to a third party, be they parent, potential employer, employer, professional body, sponsor, etc., without the consent of the individual concerned.

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

Limitations on the use of personal data for research

All researchers, be they students or staff, involved in collecting personal data, especially sensitive personal data, must comply with the requirements of the DP Acts. Initially, they must ensure that data are obtained and processed fairly. It is essential that the necessary consent from data subjects is obtained. Whenever possible, personal data should be rendered anonymous.

The DP Acts require that personal data shall be kept only for one or more specified, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those. This restriction may limit the usefulness of data for research purposes. If personal data are made anonymous, however, they cease to be personal data and are no longer subject to the terms of the DP Acts.

In addition, certain Data Protection rules are relaxed for personal data kept for statistical or research purposes, so long as the data are not used in a way that may harm the data subject. The rules in question are the restrictions on further processing personal data which is incompatible with the original purpose, on not keeping data longer than necessary for the purpose and on not disclosing the purpose when the data were obtained. It should be noted that if research data are retained in personally identifiable format it may be subject to an access request from a data subject and is subject to restrictions on the transfer of data outside the European Economic Area.

Right of rectification or erasure

Data subjects have a right to have personal data rectified or, blocked from being processed or erased where the Data Controller has contravened the DP Acts.

In order to comply with the above rights of access, rectification or erasure, ensure that personal data can be located and collated quickly and efficiently. The following guidelines should be followed in this respect:

- Ensure personal data are in a format that is easy to locate and collate.
- Verify that the access request and the personal data released refer to the same individual.
- Know exactly what data are held on individuals, and by whom.
- Hold personal data in a secure central location.

Responsibilities of data subjects

- All staff, students and other data subjects are entitled to be informed how to keep their personal data up-to-date

- All staff, students and other data subjects are responsible for:

    - Checking that any information that they provide to DIT is accurate and up to date;
    - Informing DIT of any changes of information which they have provided, e.g. changes of address;
    - Checking the information that DIT sends out from time to time, giving details of information kept and processed;
    - Informing DIT of any errors or changes (DIT cannot be held responsible for any errors unless previously informed).

Section 3: Data Classification and Data Handling Responsibilities

Based on the Data Protection Acts 1988 and 2003, the FOI Act 2014, and the Data Protection Commissioner Code of Practice:

Data Classification	**Description**	**Data Owner & Decision Maker**	**Data Handling Responsibilities**				
			Collection	**Storage**	**Transmission**	**Processing**	**Destruction**
Public Non-Personal Data	DIT information which is not prohibited by law to publish.	Head of Function	N/A	N/A	By the appropriate Head of Function	N/A	N/A
Private Non-Personal Data	DIT information which is subject to a confidentiality agreement, or the concerns financial, commercial, or intellectual property matters the disclosure of which would cause material loss.	Head of Function	As authorised by the Appropriate Head of Function.	• Physical documents subject to physical security in locked storage. • Computer data subject to IS security password or encryption.	• Physical documents transmitted with physical security measures, by informed employees, or courier firms with confidentiality agreements with DIT. • Computer data only emailed subject to IS security or encryption.	• On the authority of the appropriate Head of Function. • By third parties on the authority of the appropriate Head of Function, and subject to a confidentiality agreement.	• Data is destroyed on Authorisation of Head of Function. • Function's Data or Records Retention Schedule is updated on destruction.

Data Classification	Description	Data Owner & Decision Maker	Collection	Storage	Transmission	Processing	Destruction
Personal Data	DIT data relating to a living individual who may be identified from the data.	Head of Function	• Collected with the consent of the Data Subject (relevant individual) for the specified lawful purpose intended. • Ensure data collected is adequate, relevant, not excessive, and retained no longer than necessary for the specified purpose.	• Subject to appropriate physical locked storage and IS security password or encryption. • Subject to Data Access Request from the Data Subject (relevant individual). • Subject to being kept accurate and up to date. • Subject to retention for no longer than is necessary for the consented specified purpose.	• Data is transmitted only as necessary for the purpose it was collected. • Physical documents transmitted with physical security measures, by informed employees, or courier firms having confidentiality agreements with DIT. • Computer data only emailed subject to IS security password or encryption.	• Data is processed only in ways compatible for the consented purpose for which it was initially given. • On the authority of the appropriate Head of Function. • By third parties on the authority of the appropriate Head of Function, and subject to a confidentiality agreement.	• Data is destroyed on Authorisation of Head of Function when its consented purpose is fulfilled. • Function's Data or Records Retention Schedule is updated on destruction.
Sensitive Personal Data	DIT 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, personal data of a financial nature.	Head of Function					

Section 4: Personal Data Security Breach Management

4.1 Personal Data Security Breach Management Procedure and Guidelines

The purpose of these procedures and guidelines is to set out the processes that represent best practice in the event of a data security breach involving personal data or sensitive personal data (see Section 2 above for detailed definitions).

A Personal Data security breach ("data breach" in short) occurs when Personal Data is made available to one or more third parties without the consent of the data subject i.e. unauthorised access to, collection, use, disclosure or disposal of personal information.

If a staff member considers that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing the form below.

Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

There are statutory requirements on the Institute that all incidents in which personal data has been put at risk must be reported to the ODPC within 2 days of DIT becoming aware of the incident in particular circumstances.

Data breaches may occur in a variety of contexts, e.g.:

- Loss or theft of data or equipment on which data is stored (e.g. memory stick, laptop or paper records)
- Inappropriate access controls allowing unauthorised use (e.g. using unsecure passwords)
- Equipment failure
- Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
- Disclosing confidential data to unauthorised individuals
- Human error (e.g. emails being 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).

As a Data Controller DIT processes significant amounts of personal data and appropriate measures require to be taken against the unauthorised or unlawful processing and accidental loss, destruction of or damage to personal data.

It is essential that in the event of a data security breach, appropriate action is taken by DIT to minimise any associated risks as soon as possible.

Responding to a Potential Data Security Breach

In line with best practice, these guidelines outline five stages to managing a response to a breach:

Stage 1: Identification and Classification

If a staff member considers that a data security breach has occurred, this must be reported immediately to the Information Governance Officer at foi@dit.ie and your Line Manger by completing the **Personal Data Security Breach Report Form** in Section 4.2 below.

Information Services via the DIT Support Desk (phone 01 402 3123 or email support@dit.ie) should also be advised of the potential breach.

The Information Governance Officer will initially review the incident, as reported, and if a data security breach has occurred involving personal data or sensitive personal data they will liaise with the President who will decide if a Breach Management Group of relevant DIT stakeholders and a Chair should be appointed to investigate.

The Breach Management Group may include, amongst others as appropriate, the relevant Director or Head of Function, the Person reporting the incident, Information Services, Public Affairs and the Information Governance Officer).

Any records relating directly to an investigation by the Breach Management Group will be retained by the Information Governance Officer.

Stage 2: Containment and Recovery

Containment involves limiting the scope and impact of a data security breach. If a breach has occurred, appropriate action will be taken by the relevant DIT stakeholders to minimise any associated risks which may include:

- Establishing who within DIT needs to be made aware of the breach and ensuring relevant staff are informed what is required to assist in the containment exercise;
- Establishing whether there are any actions which may recover losses and limit the damage the breach can cause;
- Where appropriate, informing the Gardaí.

Stage 3: Risk Assessment

In assessing the risk arising from a data security breach, the relevant DIT stakeholders require to consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

The information provided at Stage 1 by the individual reporting the breach can assist with this stage.

Stage 4: Notification of Breaches

In accordance with the Office of the Data Protection Commissioner's (ODPC) "Personal Data Security Code of Practice", all incidents in which personal data has been put at risk must be **reported to the ODPC within 2 days of DIT becoming aware of the incident.**

Incidents do not have to be reported to the ODPC only when:

- The personal data concerned is protected by a DIT Information Services Department approved encryption solution1 and the password is not stored with the device

Or

- The full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and**
- It affects no more than 100 data subjects **and**
- It does not include sensitive personal data or personal data of a financial nature2.

The decision to report a breach to the ODPC will be made by the group of relevant DIT stakeholders investigating the incident.

However, if issues are raised relating to the adequacy of technological risk-mitigation measures, DIT will automatically report the incident to the ODPC.

If a decision is made by the group not to report a breach, a brief summary record of the incident with an explanation of the basis for not informing the ODPC will be retained by the Information Governance Officer.

Stage 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the relevant DIT stakeholders will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Subsequent to each data security breach a log will also be maintained by the Information Governance Officer of the agreed steps arising from each incident and this will be presented by way of an overall annual report to the President or his nominated Committee.

[1] Further information on encryption is available in DIT's Information Services IT Security Policy P: Cryptography

[2] Personal data of a financial nature means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

4.2 Personal Data Security Breach Report Form

As a matter of urgency when a Personal Data security breach has occurred please complete this form and return it to the Information Governance Officer at foi@dit.ie and your Line Manger.

The requirement in Stage 4 above that all incidents in which personal data has been put at risk must be reported to the ODPC within 2 days of DIT becoming aware of the incident is relevant here.

1.	Details of the data breach	
2.	Date and time incident occurred	
3.	Date and time incident detected	
4.	What type of data is involved?	
5.	Does data fall under the definitions of personal data and / or sensitive personal data outlined in Section 3?	
6.	Details on how the personal data was held (e.g. laptop, memory stick, personal digital assistant etc.)	
7.	Details of safeguards if any that would mitigate the risk if personal data has been lost or stolen. (e.g. encryption)	
8.	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)	
9.	Details of the number of individuals whose personal data is at risk (i.e. how many data subjects are affected by the breach?)	
10.	Details of those whose personal data has been breached (e.g. staff, students, suppliers or third parties)	
11.	Details of what the personal data could tell a third party about the data subjects affected	
12.	Any other relevant information or details that you consider relevant	

Signed: Date:
(Name of person reporting incident)

Section 5: Data Protection Subject Access Requests

5.1 Data Protection Subject Access Request Checklist

1. Request to Establish Existence of Personal Data (under Section 3 DP Acts)

An individual may submit a request to establish whether DIT holds personal data relating to them. If this data is held, DIT must:

(i) Inform the requestor that personal data is held within 21 days.

(ii) Provide a description of the data held and the purposes for which it is held.

(iii) A fee does not apply to this type of request.

2. Subject Access Request (under Section 4 DP Acts)

(i) Ensure fee of €6.35 has been received and the request has been received in writing and confirm the requestor's identity.

(ii) Check all relevant details have been provided in order to identify the request and locate all relevant data retained.

(iii) Acknowledge receipt of request to requestor within 2 weeks of date of receipt and log request on internal database and diarise reminders in line with legislative requirements.

(iv) Instruct all applicable functions to search all manual and electronic files and databases and request that all relevant data is forwarded to the Information Governance Officer together with a written confirmation of compliance.

(v) As not all personal data may be liable for disclosure, ensure that the data is screened prior to release by all applicable functions and retain a record of the request in the Office of the Institute Secretary.

(vi) Provide the data to the requestor within the statutory timeframe, i.e. within 40 days of receipt of request. *Note: Time limit for requests relating to examinations data is 60 days and is deemed to be made at the date of first publication of results or at date of request, whichever is later.*

(vii) Ensure the requested data is provided in a form which is clear to the requestor, e.g. any codes must be explained.

(viii) If data is not held on requestor, DIT must inform them within 40 days. In this case, DIT is not obliged to refund any fees charged for dealing with the access request.

(ix) If DIT does not comply with the request or has to rectify, supplement or erase the personal data concerned, the fee must be refunded to the requestor.

3. Request To Cease Processing Personal Data On The Grounds That It Would Cause Unwarranted Damage Or Distress To The Data Subject

(i) Follow Steps (ii) to (v) above (Note: A fee does not apply to this type of request).

(ii) Request all areas processing relevant personal data to cease processing same.

(iii) Ensure written confirmation of compliance is provided to the Information Governance Officer.

(iv) Confirm, in writing, to requestor within 40 days that processing of relevant data has ceased.

4. Request From Customer / Employee / Supplier To Correct, Block Or Erase Their Data

(i) Follow Steps (ii) to (v) above (Note: A fee does not apply to this type of request).

(ii) Advise all areas holding the relevant data on the requestor what is to be corrected, blocked or erased and request that this is actioned immediately.

(iii) Ensure written confirmation of compliance is provided to the Information Governance Officer.

(iv) Confirm, in writing, to the requestor within 40 days that their data has been corrected / blocked / erased.

5.2 Subject Access Request Form

Request for a copy of Personal Data

Under Section 4 Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Subject Access Request Form

Note: A fee of €6.35 and a copy of proof of identity (e.g. passport or driver's licence) must accompany this completed form.

1. Details of Requestor:

Surname: _____

Postal Address: _____

_____

Telephone / Email:

2. Details of Request:

I, _____, wish to have access to personal data that I believe DIT retains on me as outlined below: (Please include Student Number or Staff Number if relevant)

_____
_____
_____
_____
_____
_____

Signed: _____ **Date:** _____

Please return the completed form together with the relevant fee and a copy of proof of identity by post to: Information Governance Officer, Office of the Institute Secretary, Dublin Institute of Technology, 143-149 Lower Rathmines Road, Rathmines, Dublin 6, D06 H328 or by email to foi@dit.ie

For Office Use:
Date Received: _____ Date of Response to Requestor: _____

Section 6: Records Management Principles

6.1 Creating a Records Retention Schedule

- The Head of Function is required to ensure that records / data retention schedules for records and data held in their area are created that define the length of time that specified types of records and data are to be retained as well as their final disposition and method of disposition.
- The Head of Function may delegate this responsibility to a member of staff in their area who is responsible for classifying and handling data and generating guidelines for its lifecycle management. These are usually the officers responsible for the initial collection / input and use of the data and synonymous with the “record owner” or the “information owner.”
- Following approval by the Head of Function, the schedules are to be forwarded to the Information Governance Officer who will review and liaise with the relevant area on any queries.
- Once all queries have been resolved, the Information Governance Officer will arrange for the retention schedules to be noted by the Senior Leadership Team and publish the schedules on the DIT website.

6.2 Reviewing a Records Retention Schedule

- The Head of Function is responsible for ensuring that reviews of retention schedules are carried out on a regular basis and in light of any legal or other relevant indicators.
- Changes to the retention schedules are to be advised directly to the Information Governance Officer together with reasonable justification of the change, e.g. information on relevant legislation, policy changes, working practice changes etc.
- The Information Governance Officer will review the revised schedule and update the schedules on the DIT website.
- Significant changes to the schedule may require to be noted by the Senior Leadership Team.

6.3 Disposition of Records / Data

- After the records and data have been retained for the requisite time set out in the retention schedules, the Head of Function is responsible for ensuring that these are either destroyed securely by means of secure shredding or stored for the requisite period or permanently in an appropriate DIT storage area utilising the Disposition of Records / Data Register.

6.4 DIT Records Retention Schedules

Within the Institute Record Retention Schedules are already in place and currently available in the following areas:

1. Buildings
2. Employee Assistance
3. Financial Management & Accounting
4. Governing Body
5. HR (incl. Health & Safety and Staff Training & Development)
6. Information Services
7. Internal Audit
8. Library Services
9. Payroll
10. Procurement
11. Property & Facilities
12. Records Management
13. Research & Enterprise
14. Student Disciplinary Records
15. Student Records.

6.5 Records / Data Retention Schedule Form: (Name of Function)

This schedule has been reviewed by the (Insert Title of Head of Function) in light of experience and any legal or other relevant indications as follows:

1. Records / Data Group	2. Records / Data Description	3. Data Classification	4. Records / Data Retention Period	5. Records / Data Rationale for Retention	6. Records / Data Final Disposition	7. Records / Data Owner

Date Approved by Head of Function	
Date Reviewed by Information Governance Officer	
Date Noted by SLT	
Date of Last Review	

1 Records / Data Group: Specify Records / Data Group, e.g. Staff Files, Student Exam Results etc. 2. Records / Data Description: Description of files, e.g. Interview notes, minutes of meetings etc. 3. Data Classification: See across* 4. Records / Data Retention Period: Length of time which records / data should be retained for 5. Records / Data Rationale for Retention: Justification for retention period e.g. statutory requirement / operational requirement etc. 6. Records / Data Final Disposition: Action when records / data exceeds retention date i.e. archive or destroy confidentially 7. Records / Data Owner: Position holder responsible for the records / data	***3 Data Classification**	**Description**
	Public Non-Personal Data	DIT information which is not prohibited by law to publish.
	Private Non-Personal Data	DIT information which is subject to a confidentiality agreement, or the concerns financial, commercial, or intellectual property matters the disclosure of which would cause material loss.
	Personal Data	DIT data relating to a living individual who may be identified from the data.
	Sensitive Personal Data	DIT 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, personal data of a financial nature.

6.6 Disposition of Records / Data Register Form

Part I: Authorisation for Disposition of Records / Data

Function (Area / Office): _____ Proposed Destruction Date: _____

Record / Data Group	Records / Data Description	Volume of Records / Data	Disposition by: Archive / Transfer / Destruction	Reason for Disposition

I certify that the above listed records / data may be disposed of in line with DIT's Records / Data Retention Schedule:

Signature: _____ Date: _____

Print Name: _____ Position: _____
(Head of Function)

Part II: Records / Data Destruction Certificate *(Please complete if records / data are to be destroyed)*

I certify that the above listed records / data were confidentially destroyed on _____ *(Insert Date of Destruction)*

Signature: _____ Date: _____

Print Name: _____ Position: _____