DATA PROTECTION PROCEDURES

This Data Protection Procedures document applies to staff of the Institute, students of the Institute who might have reason to collate, handle and use data as part of their studies and/or research and external bodies that processes personal data on behalf of the Institute.

Document Location Freedom of Information / DP Office

Revision History

Date of this revision: Compilation date 9 January 2017	Date of next review: 9 Jan 2019

Version Number/Revision Number	Revision Date	Summary of Changes
1.0	9 Jan 2018	
2.0	Aug 2017	Procedure Guidelines to apply to staff and students

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
0.1	Jan 2017		1st draft of policy written
0.2	Aug 2017	FAR	1st draft

Approval

This document requires the following approvals:

Name	Title	Date
Peter McGrath	VP Finance and Corporate Affairs	January 2017
Governing Body		August 2017

These procedures have been approved by the Institute Management. Any additions or amendments to this or related policies will be submitted by the Data Protection Officer for approval or to whatever authority Executive Board may delegate this role. These procedures will be reviewed annually by the Data Protection Officer who will consult as necessary before submitting any amendments for approval.

1. Purpose of Data Protection

The Data Protection Act 1988, 1995 Directive and the Data Protection (Amendment) Act 2003 govern the processing of all personal data. (Data Protection Regulation Directive 2018 will largely replace the 1995 Directive and DP Acts 1988 and 2003).

The purpose of these Acts is to safeguard the privacy rights of living individuals regarding the processing of their personal data by those who control such data. In particular, it provides for the collection and use of data in a responsible way, while providing against unwanted or harmful uses of data.

2. Purpose of the compliance guidelines

The purpose of these procedures is to assist Institute employees in supporting the Institute's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with the legislation. The guidelines set out the areas of work in which data protection issues arise, and outline best practice in dealing with these issues. These guidelines should be read in conjunction with the Institute's Records Management Policy, DP Policy, Breach Management Procedures, Guidelines for Staff and Data Governance Policies and Procedures.

3. Explanation of Terms

- **Data** means information in a form that can be processed. It includes both **automated data** and **manual data.**
  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 it form part of a system.
  Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

- **Personal data** means data, including **sensitive personal 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 Institute.

Sensitive personal data relates to specific categories of data, which are defined as data relating to a person's racial origin; political opinions or religious or philosophical beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

- **Data controller** is a body that processes information about living people. The Data controller must be in a position to control the contents and use of a personal data file.

- **Data processor** is a body that processes personal data on behalf of a Data controller.

- **Processing** means performing any operation or set of operations on data, comprising:
    - obtaining, assembling, organising and storing data;
    - using, consulting and retrieving data;
    - altering, erasing and destroying data; or
    - disclosing data.

4. Role of Data Protection Commissioner

The Data Protection Commissioner, with whom the Institute is registered as a data controller, oversees compliance with the terms of the legislation. The Commissioner has a wide range of enforcement powers, including investigation of Institute records and record-keeping practices. A data controller found guilty of an offence can be fined up to €100,000 and/or may be ordered to delete data.

5. Rules of Data Protection

There are eight 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 only for one or more specified and lawful purposes;
3. use and disclose only in ways compatible with the purposes for which it was initially given;
4. keep safe and secure;
5. keep accurate, complete and up-to-date;
6. ensure that it is adequate, relevant and not excessive;
7. retain no longer than is necessary for the specified purpose or purposes;
8. provide a copy of his/her personal data to any individual, on request.

In addition, there are special conditions that must be met before personal data may be transferred to a country outside the European Economic Area (E.U. member states and 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 personal computer-held data and to all personal manual data created from the 1 July 2003. However, for manual records created before 1 July, 2003, the obligations:
- to keep data accurate, complete and up-to-date;
- to ensure that they are adequate, relevant and not excessive; and
- to retain them no longer than is necessary for the purpose or purposes
will only apply from 24 October, 2007.

Until that date the following procedures will apply to personal manual data created before 1 July, 2003:

- provide a copy of his/her personal data to any individual on request;
- correct, erase, or destroy any manual personal data that are incomplete or inaccurate;

- destroy any personal manual data that are incompatible with the legitimate purpose for which they were collected.

6. Application of the rules of data protection

In order to ensure Institute compliance with these rules, you must observe the following procedures at all times.

Obtaining and processing personal data

Personal data is obtained fairly if the data subject is aware of the purpose for which the Institute is collecting the data, 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 express purpose and ensure data are used only for that purpose.
- The use of Institute data processing facilities in capturing and storing personal data for non-Institute purposes must not take place.
- It is imperative to inform data subjects of what personal information is held by the Institute, 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 the consent. Consent cannot be inferred from non-response in the case of sensitive data.
- Remember: the data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed.

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 normally require explicit consent. Remember to anonymize data where possible and as appropriate.

- 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 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 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 Gardai 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 interests of the data subject.

- 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 EEA 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 Acts provide for disclosures, other than to the data subject, where data are:

- authorised for safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- required to protect the international relations of the State;
- required urgently to prevent damage to health or serious loss/damage to property;
- required under law;
- required for legal advice or legal proceedings;
- disclosed to the data subject;
- disclosed at the request or with the consent of the data subject;

Securing personal data

The Institute must protect personal data from unauthorised access when in use and in storage and the data must be protected from inadvertent destruction, amendment or corruption.

- Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, backup, etc.
- Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.
- Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.
- Subject to retention guidelines, personal manual data should be destroyed by confidential shredding when the retention period has expired. (Records Management Schedule)
- When upgrading or changing your personal computer, ensure the hard drive is cleaned by an appropriate IT staff member.
- Special care must be taken where laptops, personal computers and memory sticks containing personal data are used outside the Institute.
- Shared drives must be kept up to date and accessible only by personnel who need to work on those files.
- Health and social work personal data can only be released following consultation with the relevant professional.
- Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and kept up-to-date. It is recommended that

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. When collecting data ask the following questions:

- What is our specific purpose in acquiring this data?
- What is the minimum range of personal data we require for that purpose?
- Where will we source this data?
- How will we clearly state our intended purpose?
- How long will we keep the data?
- In what way can my data management decisions bring the organisation into non-compliance?
- Can we demonstrate / document our compliance?
- What are the risks to which the data might be exposed?
- What measures are we taking to protect the data against such risks?

The golden rule to always ask yourself is – Would the data subject be surprised by the use of their data?

School/Department/Function Procedures need to be reviewed on a regular basis so that if a Subject Access Request were received it can be dealt with in an expedient manner. Ask yourself the following questions:

- How would my Department react if it received a request from a data subject wishing to exercise their rights under Data Protection legislation?
- How long would it take me to collate (and correct or delete) the data from all locations where it is stored?
- Who will make the decisions about deletion/amendment?
- Can our systems respond to the data portability provision as set out in the GDPR of 2018 if applicable where we have to provide data electronically and in a commonly used format?

Disposal of personal data

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

Rights of data subjects

Right of access

The 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 40* calendar 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 the him or her, unless given in confidence.

A maximum fee of €6.35* may be charged.

(See also How to Make a Subject Access Request document)

**The new General Data Protection Regulation coming into force in May 2018 reduces the time considerably to 20 days and abolishes the fee. There should be no undue delay in processing an Access Request and at the latest must be concluded within one month.*

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 the Institute 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. The Institute should not engage in ‘mail hosting’ which is not relevant to its purposes.

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 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. All data collected must also follow the DkIT Ethics Procedures/Policy.

The 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 subject to the terms of the Acts.

In addition, certain data protection rules are relaxed for personal data kept for statistical, research or other scientific purposes, so long as the data are not used in a way that may harm the data subject. The rules in question being the restrictions on further processing personal data that 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 they may be subject to an access request from a data subject and are 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 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:

- 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 should be informed of how to keep their personal data up to date.
- All staff, students and other data subjects are responsible for:
    - checking that any information that they provide to the Institute is accurate and up to date;
    - informing the Institute of any changes in information that they have provided, such as changes of address;
    - checking the information the Institute sends out from time to time, giving details of information kept and processed;
    - informing the Institute of any errors or changes (the Institute cannot be held responsible for any errors unless previously informed).

7. Further information

These guidelines are intended as a general introduction and are not an authoritative interpretation of the law. Extensive information is available from the Data Protection Commissioner's website, www.dataprotection.ie or from the Office of the Data Protection Commissioner, Canal House, Station House, Portarlington, Co Laois.

If you have any queries or require clarification on any aspect of this document, please contact Ms Loretto Gaughran, Freedom of Information Officer on Tel 042 93 70222 or email loretto.gaughran@dkit.ie

Note: The term 'Institute' is used for brevity in this document but should be taken as referring to the Dundalk Institute of Technology.