Institiúid Teicneolaíochta Cheatharlach

INSTITUTE of TECHNOLOGY CARLOW

At the Heart of South Leinster

Data Protection Policy

Effective Date	March 2013	**Version**	01
Approved By	Senior Management	**Date Approved**	15th March 2013

Form(s)	Responsibilities/ Owner
	Registrar Secretary/Financial Controller FOI/Data Protection Officer
Superseded or Obsolete Procedures NIL	

1. Introduction

In accordance with the functions outlined in the Regional Technical Colleges Act and the Institutes of Technology Act, the Institute of Technology Carlow (ITC) is required to collect, use and keep personal data (information) for a variety of purposes about its staff, students and other individuals who come in contact with the Institute. The purposes of processing data about staff, students and other individuals with whom ITC has dealings include *inter alia* 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.

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data. The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 (the DP Acts) confer rights on individuals as well as responsibilities on those persons processing personal data. Personal data, both automated and manual, are 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 (for the purposes of this policy, the Data Controller is ITC). Under regulations introduced by the Minister for Justice, Equality and Law Reform on 1st October 2007, ITC 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. ITC is, however, still obliged to comply with the general provisions of the DP Acts.

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.

2. Purpose of this Policy

This policy is a statement of ITC's commitment to protect the rights and privacy of individuals in accordance with the DP Acts.

3. Definitions used in the DP Acts

The following definitions have been adapted from Section 1 of the DP Acts:

- ***Data*** means automated 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 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.

4. Data Protection Principles

As a Data Controller, ITC must comply with the eight Data Protection Principles which are set out in the DP Acts and will administer its responsibilities under the legislation in accordance with these stated principles as follows:

(i) *Obtain and process information fairly*
ITC will obtain and process personal data fairly and in accordance with its statutory and other legal obligations.

(ii) *Keep data only for one or more specified, explicit and lawful purposes*
ITC will keep personal data for purposes that are specific, lawful and clearly stated and the personal data will only be processed in a manner compatible with these purposes.

(iii) *Use and disclose of data only in ways compatible with these purposes*
ITC will only use and 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*
ITC 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.

(iv) *Keep data accurate, complete and, where necessary, up-to-date*
ITC will have procedures that are adequate to ensure high levels of data accuracy and will put in place appropriate procedures to keep data up-to-date.

(v) *Ensure that data are adequate, relevant and not excessive*
Personal data held by ITC 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*
ITC has a policy on retention periods for personal data which is contained in the Institute's Records Management Policy and its related appendices.

(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*

ITC will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

5. Responsibility

ITC has overall responsibility for ensuring compliance with the Data Protection legislation when it is the data controller of personal data. However, all employees and students 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. The Institute will provide support, assistance, advice and training to all sections, offices and staff to ensure it is in a position to comply with the legislation.

It will be the responsibility of all managers to develop and encourage good information handling practice within the Institute.

While ITC is the Data Controller under the DP Acts and is therefore ultimately responsible for their implementation, in order to handle day-to-day matters, the Institute has appointed an officer who will assist the Institute and its staff with compliance with the DP Acts.

Each manager must ensure that the officer is informed of any changes in uses of personal data that might affect ITC's compliance with the DP Acts.

6. Procedures and Guidelines

This policy supports the provision of a structure to assist in the Institute's compliance with the DP legislation. This structure includes best practice guidelines and procedures in relation to all aspects of Data Protection.

7. Procedure for obtaining personal data (Right of access)

Under section 4 of the Data Protection Acts, an individual has the right to request a copy, of certain information relating to them kept on computer or in a structured manual filing system by any person or organisation.

A request under section 4 must be in writing, should be addressed to the Data Compliance officer and should include any additional details that may be necessary to enable the organisation to locate the requested record; e.g. customer account number, staff number, or RSI number (if the request is to a public-sector organisation). A fee may be charged, but this cannot exceed €6.35.

Once a request is made, and appropriate fees paid (if any), the request will be considered and a response will be provided to the requester within 40 days.

8. Exceptions to the Right of Access

Sections 4 and 5 of the Data Protection Acts set out circumstances in which the right of an individual to obtain access to their personal records can be limited.

This is necessary in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand. For example, a criminal suspect does not have a right to see the information held about him by An Garda Síochána, where that would impede a criminal investigation; and you do not have a right to see communications between a lawyer and his or her client, where that communication would be subject to legal privilege in court.

Section 4(6) of the Acts set out the restrictions regarding the right to obtain access to examination results.

9. Status of this Policy

This Policy applies to all staff and students of the Institute. Any breach of the DP Acts or this Policy will be taken seriously and may result in disciplinary proceedings.

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 Manager in the first instance.

10. Review

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