CIT Institiúid Teicneolaíochta Chorcaí
Cork Institute of Technology

CORK INSTITUTE OF TECHNOLOGY

DATA PROTECTION POLICY

APPROVED BY GOVERNING BODY ON 30 APRIL 2009

INTRODUCTION

Cork Institute of Technology is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

The Institute needs to process personal data about its staff, students and other individuals with whom it has dealings for administrative purposes which include;

- Recruitment and payment of staff
- Organisation and administration of courses
- Academic Quality Assurance, Evaluation and Examination
- Research activities
- Compliance with statutory and legal obligations
- Procurement and Purchasing

To comply with the law, personal data must be collected and used fairly, stored securely and not disclosed to any third party unlawfully.

Policy Objective

To ensure the Institute complies with the Data Protection Acts

To ensure compliance by the Institute with the eight principles of data protection as set down by the Data Protection Commissioner based on the Acts.

To ensure that the data protection rights of students, staff and others are safeguarded.

Principles of the Act

The Institute will administer its responsibilities under the legislation in accordance with the eight stated Data Protection principles outlined in the Act as follows;

1. Obtain and process information fairly
   The Institute will obtain and process personal data fairly and in accordance with the fulfilment of its functions.

2. Keep it only for one or more specified, explicit and lawful purposes
   The Institute 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.

3. Use and disclose it only in ways compatible with these purposes
   The Institute will only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

4. Keep it safe and secure
   The Institute will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The Institute is aware that high standards of security are essential for all personal information.

5. Keep it accurate, complete and up-to-date
   The Institute will have procedures that are adequate to ensure high levels of data accuracy. The Institute will examine the general requirement to keep personal data up-to-date. The Institute will put in place appropriate procedures to assist staff in keeping data up-to-date.

6. Ensure that it is adequate, relevant and not excessive
   Personal data held by the Institute will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

7. Retain it for no longer than is necessary for the purpose or purposes
   The Institute will have a policy on retention periods for personal data.

8. Give a copy of his/her personal data to that individual, on request
   The Institute will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

Responsibilities

The Institute has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees 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 departments, offices and staff to ensure it is in a position to comply with the legislation. The Institute has appointed a Data Protection Officer who will assist the Institute and its staff in complying with the Data Protection legislation.

Procedures and Guidelines

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

Procedures for obtaining personal data (Right of access)

Under the Data Protection Acts, an individual has the right to request a copy of certain information relating to them held on computer, paper or other manual form by any person or organization.

A request must be in writing, (click here for application form), should be addressed to the Data Compliance Officer and should include any additional details that may be necessary to enable the organization to locate the requested records.

Once a request is made, and appropriate fees paid (a fee may be charged but cannot exceed EUR6.35), the request will be considered and a response will be provided to the requester within 40 days.

Exceptions to the Right of Access

Individuals have a strong right of access to see their personal data. However, section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply.

1. If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities Comment: It would obviously be unacceptable to allow a criminal suspect to see all of the information kept about him by An Garda Síochána, where this would be likely to impede the effectiveness of the criminal investigation. On the other hand, however, if allowing an individual access to personal information about him or her would not be likely to impede an investigation, then the access request would have to be complied with.

2. If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention

3. If the information is kept for certain anti-fraud functions: but only in cases where allowing the right of access would be likely to impede any such functions

4. If granting the right of access would be likely to harm the international relations of the State

5. If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation

6. If the information would be subject to legal professional privilege in court

7. If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved

8. If the information is back-up data.
   Comment: It would be unreasonable to expect an organisation to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way.

Examinations Data

Section 4(6) of the Data Protection Act makes special provision for responding to an access request about the results of an examination. "Examination" in this context means any test of knowledge, skill, ability etc., and is therefore not confined to official State examinations. Medical examinations are not covered, though. These special rules

(a) increase the time limit for responding to an access request from 40 days to 60 days, and

(b) deem an access request to be made at the date of the first publication of the examination results or at the date of the request, whichever is the later.

Definitions

The following definitions are as per the Data Protection Acts 1998 and 2003. For a full copy of the Data Protection Act 1998 please click here or, for the Data Protection (Amendment) Act 2003 click here.

Personal Data

This 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.

Sensitive Personal Data

This means personal data as to –

a) The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.
b) Whether the data subject is a member of a trade union.
c) The physical or mental health or condition or sexual life of the data subject.
d) The commission or alleged commission of any offence by the data subject.
e) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal if such proceedings or the sentence of any court in such proceedings.

March 2009