Dublin City University

ICT Compliance Policy

Contents

Compliance Policy 1
Data Protection 1
Freedom of Information 1
Copyright and Intellectual Property: 2
Electronic Commerce Act, 2000, eCommerce Directive (2000/31/EC) and European Communities (Directive 2000/31/EC) Regulations 2003 2
European Communities (Data Protection) Regulations 2001 4
European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002 as amended by SI 526 of 2008..... 4
Child Trafficking and Pornography Act: 6
Criminal Damages 6
HEAnet Acceptable Use Policy 6
Code of Conduct for the Use of Computing Resources within DCU 7
Breaches of the Code of Conduct 7
Document Change Management 8
Appendix 1- Relevant Legislation, Policies and Procedures i

Compliance Policy

The University has an obligation to abide by all applicable Irish and European legislation together with organisational policies and procedures. A list of relevant legislation and policy/procedures are provided in Appendix 1.

Data Protection

The Data Protection Acts safeguard the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The terms of the Data Protection Acts 1988 and 2003 lay down strict rules about the way in which personal data is collected, accessed, used and disclosed. The terms of the legislation also permit individuals to access their personal data on request, and confers on individuals the right to have their personal data amended if found to be incorrect. All users of DCU's information computing technology must comply with the current legislature.

Freedom of Information

The main objective of the Freedom of Information Act is to foster and develop a culture of openness, transparency and accountability in public bodies. The Act confers three new *legal* rights on individuals:

1. The right to obtain information held by the University.
2. The right to obtain reasons for decisions affecting oneself.
3. The right to have official information relating to oneself amended where it is incorrect, incomplete or misleading.

This means that apart from information already published or otherwise available, individuals may apply:

- for access to university records retrospectively to the date the Act was implemented, which was 21 April 1998;
- for access to records that contain personal information about them irrespective of when created;
- for access to their own personnel records created since 21 April 1995;
- to have made known to them the reasons for decisions made by the university that have materially affected them. This right is effective from 22nd October 2001.

Copyright and Intellectual Property:

Most material (including software such as programs, audio, video, data files, etc.) that is publicly available (including on the Internet) is subject to copyright or other intellectual property right protection.

When obtaining material for use inside or outside of DCU:

- Do not obtain material from sources for use within or outside of DCU unless express permission to do so is stated by the material owner.
- You must read and understand any copyright restrictions relating to the material. If you think that DCU will not be able to comply with any part of the terms, do not download or use the material.
- Ensure that you comply with any expressed requirements or limitations attached to the use of such material (for example: must not be used for commercial purposes; cannot charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy; must distribute source code; etc.).

http://www.irishstatutebook.ie/1998/en/act/pub/0028/index.html

Electronic Commerce Act, 2000, eCommerce Directive (2000/31/EC) and European Communities (Directive 2000/31/EC) Regulations 2003

The purpose of the Regulations is to create a legal framework in Ireland so as to ensure the free movement of information society services between Ireland and EC & EEA. An Irish service provider who provides his services in another member state must comply with Irish Law (sometimes referred to as the "single market principle" or "country of origin rule"). This does not apply in the following cases:

- Protection of consumers and investors;
- Prevention or detection of crime;
- National security;
- Protection of minors;
- Protection of public health.

The Regulations do not apply inter alia to:

- The Collection of taxes;

- The representation of a party to legal proceedings;
- Gambling.

The main provisions of the Electronic Commerce Act are as follows:

- Information (such data, writing or other text) cannot be denied legal effect, validity or enforceability simply because it is in electronic form (Section 9);
- Where a person is required by law or contract to give information in writing then, in general, this may be given in electronic form by e-mail or otherwise. This would include making an application or request, lodging a claim or return and recording and disseminating a court order (Section 12).
- Where law or contract requires a person, to sign a document, then this may be given in electronic form. (Section 13).
- Contracts law or contract requires a person, to sign a document, then this may be given in electronic form. (Section 13).
- The law or contract requires a person, to sign a document, then this may be given in electronic form. (Section 13).
- Advanced Electronic Signatures', such as public key systems that utilise encryption, may be used for witnessing signatures or sealing documents (Section 14 & 16).
- If information is required to be kept in its original form, by law or contract, then it may be kept in electronic form. This is provided that its integrity and accessibility is assured (Section 17).
- If information is required to be retained or produced, by law or contract, this may be done in electronic form (Section 18).
- The Act contains provisions on the dispatch and receipt of electronic communications (Sections 20 & 21).
- The Act gives the Minister for Public Enterprise power to prohibit and regulate the registration of the i.e. domain name within Ireland (Section 31).
- Defamation law will apply on-line (Section 23).
- Consumer law will apply on-line (Section 15).
- Nobody can be forced to use electronic signatures as a result of the Acts provisions (Section 24).

http://www.irishstatutebook.ie/2000/en/act/pub/0027/index.html

http://www.irishstatutebook.ie/2003/en/si/0068.html

European Communities (Data Protection) Regulations 2001

The Regulations provide that organisations may not transfer personal data to third countries which do not have an adequate standard of data protection - unless the organisation can point to other safeguards to protect people's privacy. Such safeguards could include appropriate contractual provisions, or the clear consent of the individuals in question. The EU Commission issues rulings regarding the adequacy of data protection levels in third countries, and regarding appropriate "model contracts" which organisations may use. Where the EU Commission has not made a ruling on such matters, the Data Protection Commissioner may be called upon to authorise a particular transfer of personal data, or to authorise particular types of transfer.

The Regulations also implement Article 17 of the Data Protection Directive, dealing with security measures for processing personal data. The Regulations clarify that data controllers must put in place appropriate security provisions for the protection of personal data, having regard to the current state of technological development, the cost of implementing security measures, the nature of the personal data, and the harm that might result from unauthorised processing or loss of the data concerned. The Regulations clarify the territorial application of Irish data protection law to data controllers established in the State, and to data controllers established outside the EEA who process data in the State. Data controllers in the latter category must designate a representative in the State.

http://www.dataprotection.ie/documents/legal/6si626-01.htm

European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002 as amended by SI 526 of 2008.

The Regulations lay down detailed rules which must be complied with by telecommunications companies and by companies using telecommunications and electronic communications networks for direct marketing. Companies who fail to comply commit a criminal offence that can be prosecuted by the Data Protection Commissioner. Each unlawful marketing message or call constitutes a separate offence which can attract a fine of €5,000 on summary conviction. If convicted

on indictment, the fines range from €50,000 for a natural person to €250,000 or 10% of turnover if the offender is a corporate body.

The Regulations set out the data protection standards that apply in the case of public telecommunications networks – including issues of security, privacy and direct marketing. The main features of the Regulations fall into seven categories, as follows:

1. Retention of detailed telephone records

Detailed records of people's telephone calls may be kept for as long as necessary to enable bills and telecommunications providers interconnect payments to be settled, but no longer. Certain companies may be specifically required to retain such details for a longer period.

2. Storing and Accessing information on terminal equipment e.g. "Cookies"

Information cannot be stored on or retrieved from a person's computer or other terminal equipment unless clear information is given to the individual and the individual has the right to refuse the placing or accessing of this information.

3. Calling Line Identification or "Caller ID"

Telephone users have the right to block their phone number, so that it is not displayed to other telephone users. Person's making direct marketing phone calls must however not conceal their phone number when making such calls.

4. Location Data

Location data, other than traffic data, can only be processed if made anonymous or with the consent of the individual for the provision of a value added service.

5. Public Telephone Directories

Individuals are to be informed about the purpose of directories. They have the right to be excluded from public phone directories, or to have their address and gender omitted to protect their privacy.

6. Direct Marketing

Unsolicited direct marketing e-mail cannot be sent to individuals unless they have given their prior consent. Individuals can sign up to a central 'opt out' register, to indicate that they do not wish to receive unsolicited telephone calls. Offenders are subject to fines of €5,000 per call or message on summary conviction. If convicted on indictment, the fines range from €50,000 for a natural person to €250,000 or 10% of turnover if the offender is a body corporate.

7. Enforcement and Compliance

The Data Protection Commissioner enforces the data protection aspects of the Regulations, and the Commission for Communications Regulation (ComReg) is responsible for ensuring compliance with some technical and practical elements of implementing the Regulations.

http://www.irishstatutebook.ie/2003/en/si/0068.html

Child Trafficking and Pornography Act:

This Act was introduced to strengthen legislation to prohibit trafficking in, or the use of, children for the purposes of their sexual exploitation and the production, dissemination, handling or possession of child pornography, and to provide for other related matters. "Child" within the Act means a person under the age of 17 years.

http://www.irishstatutebook.ie/1998/en/act/pub/0022/index.html

Criminal Damages

In summary, the Criminal Damages legislation deals with:

- Actual or threatened damage to property
- Unauthorized access to computers and
- Possession with intent to damage property

http://www.irishstatutebook.ie/ZZA31Y1991.html

HEAnet Acceptable Use Policy

HEAnet is the name given to the collection of networking services and facilities which support the communication requirements of the Irish education and research community.

HEAnet services should be used in such a way as to:

- Apply public funding only to the purposes for which it was voted
- Abide by the law of the land and
- Not conflict or override the rules and regulations of member organizations

http://www.heanet.ie/about/policy.html

Code of Conduct for the Use of Computing Resources within DCU

The University provides computing resources for use by student and staff to support the normal activities of the University, in particular for educational, research and administrative purposes.

The purpose of the Code of Conduct is to make users aware of what the University deems to be acceptable and unacceptable usage of the facilities and to provide guidelines for good practice.

Computing resources must not be used for any illegal or unethical purposes and should not generally be used for recreational or personal use.

Those acting in contravention of the Code of Conduct may be subject to the University's disciplinary procedures and/or criminal proceedings.

http://www.dcu.ie/info/regulations/computing.shtml

Breaches of the Code of Conduct

The purpose of this document is to define the processes to be followed within DCU when a breach, or an alleged breach, of the Code of Conduct has been reported.

http://www.dcu.ie/info/regulations/breaches.shtml

Document Change Management

Dublin City University believes that it is important to keep this Information Security Compliance Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.

The Director of Information Systems and Services (ISS) will draft necessary changes and have them reviewed and approved by the Executive Group of DCU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.

Appendix 1- Relevant Legislation, Policies and Procedures

(i) Data Protection Acts (1988 & 2003):
http://www.dataprotection.ie/docs/Home/4.htm

(ii) Freedom of Information:
http://www.irishstatutebook.ie/1997/en/act/pub/0013/index.html

(iii) Copyright and Related Rights Act (2000)
http://www.irishstatutebook.ie/ZZA28Y2000.html

(iv) Intellectual Property:
http://www.irishstatutebook.ie/1998/en/act/pub/0028/index.html

(v) Electronic Commence Act, 2000
http://www.irishstatutebook.ie/2000/en/act/pub/0027/index.html

(vi) European Communities (Directive 2000/31/EC) Regulations 2003
http://www.irishstatutebook.ie/2003/en/si/0068.html

(vii) European Communities (Data Protection) Regulations 2001
www.irishstatutebook.ie/2001/en/si/0207.html

(viii) European Communities (Data Protection and Privacy in Telecommunications) Regulations 2002
http://www.irishstatutebook.ie/2003/en/si/0068.html

(ix) Child Trafficking and Pornography Act(1998):
http://www.irishstatutebook.ie/1998/en/act/pub/0022/index.html

(x) Criminal Damages Act:
http://www.irishstatutebook.ie/ZZA31Y1991.html

(xi) HEAnet Acceptable Use Policy:
http://www.heanet.ie/about/policy.html

(xii) DCU Code of Conduct for the Use of Computing Resources within DCU:
http://www.dcu.ie/info/regulations/computing.shtml

(xiii) Breaches of the Code of Contact for the Use of Computing Resources within DCU:
http://www.dcu.ie/info/regulations/breaches.shtml