Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Dublin City University

Data Protection Policy

Data Protection Policy
Version 2.0

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Contents

Purpose

Dublin City University, as a Data Controller, is required by law to comply with the following Irish legislation relating to the processing of Personal Data:

- **The Data Protection Act 1988** (The Principle Act) and
- **The Data Protection (Amendment) Act 2003**

This document is the University's policy in response to the requirements of the Data Protection Acts.

Scope

In order to carry out its statutory, academic and administrative functions DCU needs to collect and process personal information relating to many categories of people, which include the students and staff of the University.

The University takes the confidentiality of all personal information particularly seriously and consequently takes all reasonable steps to comply with the principles of the Data Protection Acts. The University aims to collect personal information only in order to meet specific legitimate purposes, and to retain that information only for as long as those purposes remain valid. Ordinarily, the University will not pass personal information to any third party, except where required by law, statutory obligations or legitimate purposes balanced against the rights and interests of the data subject.

The University is committed to ensuring that all employees, registered students, agents, contractors and data processors comply with the Data Protection Acts regarding:

- the processing and confidentiality of any personal data held by the University, and
- the privacy rights of individuals under the legislation.

Data Protection Principles

To comply with the law, information (as defined by the Data Protection Acts) must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the University must comply with the following eight Data Protection Principles or Obligations:

1. **Obtain and process information fairly**
   The Data must be obtained and processed fairly and lawfully and only when certain conditions are met. (See Definition for details on conditions regarding Personal Data and Sensitive Personal Data.)
2. **Keep it only for one or more specific, explicit and lawful purposes**
   The Data can only be obtained for specified, lawful and clearly stated purposes and only processed in accordance with the University's notification to the Data Protection Commissioner.
3. **Use and disclose only in ways compatible with these purposes**
   Processing and Disclosure of personal data should not be incompatible with the specified purpose for which it was obtained.
4. **Keep it safe and secure**
   The Data must be kept safe and secure. DCU, as the Data Controller, is responsible for applying adequate security structures to prevent unlawful or inadvertent processing, alteration or loss of the data.
5. **Keep it accurate, complete and up-to-date**
   The Data must be kept accurate, complete and where necessary up-to-date.
6. **Ensure it is adequate, relevant and not excessive**
   The Data obtained should be adequate, relevant and not excessive
7. **Retain for no longer than is necessary**
   The Data should not be kept for longer than is necessary for the purpose or purposes for which it was obtained. (See also DCU's Record Retention Management Policy.)
8. **Give a copy of his/her personal data to that individual, on request**
   The Data Subject, the person to whom the information relates, has a Right of Access. The Controller must store and maintain the data in such a manner as to be able to respond to a Subject Access Request in a timely manner.

Disclosure of Personal Data

The legislation recognises two categories of Personal Data –

- 'Ordinary' Personal Data such as name, address, mobile phone number, car registration, PPS Number.
- Sensitive Personal Data, which is more deeply personal to an individual, such as their racial or ethnic background, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the (alleged) commission of any offence, subsequent proceedings or sentence.

Sensitive personal data should normally only be processed if the data subjects have given their explicit consent to this processing.

The legislation applies equally to **automated and manual data**, i.e. data held or processed on a computer, or data held in 'hard copy', stored in an indexed or relevant filing system.

The security of personal information in the possession of the University is of paramount importance and is, therefore, addressed in various policies and procedures throughout the institution. In addition to the principles contained within this policy, staff are also advised to read and adhere to the University's Data Classification Policy, Data Handling Guidelines and Contact with Third Parties Policy.

All staff and students have an individual responsibility to ensure that they adhere to the University's Data Protection Policy and the Data Protection Acts.

(Templates for a Contract for Services with Third Parties and an Agreement for the Provision of Goods and Services are available from the Procurement Office, Finance Department, DCU. Third Parties should also be made aware of the appropriate ICT Policies that they are required to adhere to.)

Summary of Responsibilities

School / Department Responsibilities

Key post holders have responsibility for ensuring that:

- All personal data being processed within the School/Unit complies with the Data Protection Acts and the University's Data Protection Policy.
- All contractors, agents and other non-permanent university staff used by the school/unit, are aware of and comply with, the Data Protection Acts and the University's Data Protection Policy.
- All personal data held within the School/Unit is kept securely and is disposed of in a safe and secure manner when no longer needed.

Staff Responsibilities

All staff must ensure that:

- Personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform the University of any errors, corrections or changes, for example, change of address, marital status, etc;

- Personal data relating to living individuals which they hold or process is kept securely;
- Personal data relating to living individuals is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- When supervising students who are processing personal data, that those students are aware of the Data Protection Rules, and the University's Data Protection Policy.

Student Responsibilities

All students must ensure that:

- Personal data which they provide in connection with their studies is accurate and up-to-date, and that they inform the University of any errors, corrections or changes, for example, change of address, marital status, etc;
- When using University's facilities to process personal data (for example, in course work or research), they notify their supervisor/advisor in the relevant department/faculty, who will provide further information about the University's policy on Data Protection compliance.

Research and Personal Data

The legislation provides certain exemptions for data collected, held and processed for research purposes (including historical and statistical purposes). If the purpose of the data processing is other than to take measures or make decisions which are targeted at particular individuals, and it does not cause substantial distress or damage, it:

- can be processed for purposes other than that for which it was collected, provided that it is still only a research purpose,
- can be held indefinitely, and
- is exempt from the Data Subject's right of access (where the data is processed for research purposes only).

The results of the research or statistics derived from the research should not be made available in a form which identifies the individuals concerned.

Personal data provided or used for research purposes does not have a blanket exemption from the Data Protection Rules. Researchers wishing to use personal data should be aware that the Data Protection Rules will still apply.

Researchers and Project Leaders must ensure that:

- employees and students are aware that, while some exemptions are granted for the use of personal data for research purposes, the majority of the Data Protection Principles must be conformed to,
- in all circumstances where personal data is to be used for research purposes, there is an adequate review in advance of processing, to ensure that the requirements of the Act can be adhered to,
- a suitable mechanism is in place to ensure that Data Subjects whose personal data is to be, or has been processed, can meaningfully exercise their right to object to the processing of that data, on the grounds that it would cause them significant damage or distress, and
- particular care is taken when the processing involves sensitive personal data.

Rights under the Acts (1988 & 2003)

The Data Subject is entitled to:

- Access to a copy of any data held by the DCU which relates to them;
- Require that any inaccurate data held by the DCU is corrected or erased;
- Prevent processing of the data likely to cause them distress or damage;
- Prevent evaluative decisions being made solely by automated means;
- Prevent processing of their personal data for the purposes of Direct Marketing;
- Request assistance from the Data Protection Commissioner's Office; and
- In the event of a breach of these rights, to pursue compensation through the Courts.

Subject Access Request (SAR)

A Data Subject is entitled to a copy of all data held by the Controller which relate to them.

To be a valid request, the SAR must be:

- Made in writing to the controller
- Provide adequate identification

On receipt of a valid SAR, the Data Controller (DCU) must comply with the request as soon as possible, but within not more than 40 days from receipt of the request.

Transfer of Data Overseas

The Data Protection Acts prohibits the transfer of personal data to any country outside of:

- The European Economic Area (EEA = EU Member States plus Iceland, Liechtenstein and Norway,);
- The 7 designated Safe Countries (Canada, Argentina, the Isle of Man, Guernsey, Jersey, the Faroe Islands and Switzerland)
- Organisations within the United States which subscribe to the 'Safe Harbour' principles.

Before transfer to any other destination, DCU, as a Data Controller, must be satisfied as to the adequacy of protection which will be provided to the data at its destination.

CCTV on the DCU Campus

DCU has closed circuit television cameras (CCTV) located throughout the campus covering buildings, internal spaces, car parks, roads, pathways and grounds. CCTV cameras are also located at the University Sports Grounds at St Clare's. This is necessary in order to protect against theft or pilferage, for the security of staff, students and visitors and for the security of DCU property.

Whilst CCTV footage is monitored by DCU security staff, access to recorded material is strictly limited to authorised personnel. The images captured are retained for between 20 and 60 days, depending on activity levels, except when the images identify an issue and are retained specifically in the context of an investigation of that issue. CCTV footage may be entered as evidence in the event of disciplinary proceedings involving staff or students. CCTV footage is not disclosed to any third party except An Garda Síochána in the case of a disclosure pursuant to Section 8 of the Data Protection Act 1988 (i.e. where it is required for the purpose of preventing, detecting or investigating alleged offences). A full list of camera locations is available on request from the Estates Office. Signage indicating that CCTV is in use is provided at the entrances to the campus. For information on CCTV operations at DCU please contact the Director of Estates.

Incorporation Programme - Sharing of Personal Data

As part of the Incorporation Programme, which involves Dublin City University Glasnevin, St. Patricks College Drumcondra, Mater Dei Institute of Education Clonliffe and the Church of Ireland College of Education Rathmines, personal data relating to staff and students of Dublin City University may be shared with these incorporating institutions. The personal data which may be shared shall be limited to that required for the purposes of the Incorporation Programme and all institutions shall be required to adhere to provisions governing the sharing of personal data as set out in the letter of agreement between the institutions involved.

FOR FURTHER INFORMATION:

Within DCU, the Data Protection Officer (DPO) has responsibility for the co-ordination of Data Protection issues including the annual registration with the Office of the Data Protection Commissioner. Queries and clarifications should be directed to the DPO.

More complete information is available from the Office of the Data Protection Commissioner at: http://www.dataprotection.ie.

This Policy document will be reviewed regularly and updated as appropriate in line with any legislative or other relevant development.

Definitions

Data	Information which is being used or held in a computerised system, or a 'relevant filing system' i.e. a manual filing system that is structured in such a way that data contained within it is readily accessible. Data can be written information, photographs, fingerprints or voice recordings.
Personal Data	Information that identifies and relates to a living individual, and includes any expression of opinion or intention about the individual. Personal data could be contact details, date of birth, qualifications, or anything pertaining to an individual. It is something that affects that person's privacy (whether in their personal/family life or business/professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and identifies that person – by itself or with other information. Personal data shall not be processed unless at least one of the following conditions is met, • The consent of the individual. • The performance of a contract with the individual. • A requirement under a legal obligation. • The protection of the individual's vital interests. • The processing is necessary - (i) for the administration of justice, (ii) for the performance of a function conferred on a person by or under an enactment, (iii) for the performance of a function of the Government or a Minister of the Government, (iv) for the performance of any other function of a public nature performed in the public interest by a person, • The processing is necessary for the purposes of the legitimate interests pursued by the data controller (DCU) or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Sensitive Personal Data	Sensitive personal data is defined as information relating to an individual's: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious beliefs or beliefs of a similar nature ▪ Membership of a trade union ▪ Physical or mental health or condition ▪ Sexual life ▪ Commission or alleged commission of an offence ▪ Proceedings for any offence or alleged offence, or sentence of court Sensitive personal data shall not be processed unless at least one of the conditions detailed in respect of personal data is met and at least one of the following conditions is also met: • The Explicit consent of the individual. • A legal obligation in the context of employment. • The protection of the vital interests of the individual. • The processing is carried out in the course of the legitimate activities by any body corporate, or unincorporated body of persons, that - (A) is not established, and whose activities are not carried on for profit, and (B) exists for political, philosophical, religious or trade union purposes. • The information has been made public by the individual. • The information is required in connection with legal proceedings. • The information is required for medical purposes. • The processing is necessary for certain public functions, e.g: • in order to obtain information for use, subject to and in accordance with the Statistics Act, 1993, only for statistical, compilation and analysis purposes, - is carried out by political parties, or candidates for election to, or holders of, elective political office in the course of electoral activities for the purpose of compiling data on people's political opinions and complies with such requirements (if any) as may be prescribed for the purpose of safeguarding the

	fundamental rights and freedoms of data subjects - the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest, - the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy or other moneys owed or payable to the State and the data has been provided by the data subject solely for that purpose, - the processing is necessary for the purposes of determining entitlement to, or control of, or any other purpose connected with the administration of any benefit, pension, assistance, allowance, supplement or payment under the Social Welfare (Consolidation) Act 1993, or any non-statutory scheme administered by the Minister for Social, Community and Family Affairs.
Processing	Anything which can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.
Data Subject	An individual who is the subject of personal data. This will include: staff, current and prospective students, graduates, suppliers of goods and services, business associates, conference delegates, survey respondents etc.
Data Controller	Refers to Dublin City University. This includes university staff who collect and process personal data on behalf of the University, and students who are collecting and processing personal data on behalf of the University or as part of their studies.
Data Processor	Any person (other than an employee of the University) who processes personal data on behalf of the University, e.g. printing agency.
Recipient	Any person or organisation to which personal data is disclosed.

Document Change Management

Dublin City University believes that it is important to keep this Data Protection Policy current in order to ensure that it addresses legislative changes and 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 University Data Protection Officer (DPO) will draft necessary changes and have them reviewed and approved by the appropriate DCU bodies. The DPO will send the proposed new policy or changes to Executive for review and approval. 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 DPO.

Version Control

Document Name	Data Protection Policy
Version Reference	2.0
Document Owner	Office of the Chief Operations Officer
Approved by	Executive
Date	2nd June 2015