

# UNIVERSITY OF ULSTER DATA PROTECTION POLICY 2009

## 1 INTRODUCTION and DEFINITIONS

The Data Protection Act 1998 (the Act) came into force on 1 March 2000 in the UK repealing previous UK legislation in this area. The purpose of the Act is to protect the individual rights and freedoms of persons especially their right to privacy with respect to the processing of personal data. Due to the nature of business at the University of Ulster (the University) it is required to hold and process, both electronically and manually, large amounts of personal data. The Act provides a framework to ensure that personal information processed and stored by the University whether in hard copy and electronic format is handled properly both on and off campus.

### 1.1 Definitions

- |       |                           |   |
|-------|---------------------------|---|
| 1.1.1 | “Data Controller”         | individuals and organisations that process personal data. The University of Ulster is a data controller.  |
| 1.1.2 | “Data Subject”            | anyone about whom personal data is held. For the University, Data Subjects include current, past and present students and staff (including affiliated and visiting staff), and other third parties such as suppliers, contractors, consultants or referees.                                       |
| 1.1.3 | “Personal Data”           | data which relates to any living individual who can be identified: from this data; or from those data and other information that is in the possession of, or is likely to come into the possession of the data controller. It includes, for example, name, date of birth, images and photographs. |
| 1.1.4 | “Processing”              | any activity that includes obtaining, recording, holding or storing personal data, and carrying out any operations on it, for example, using, disclosing, adapting, altering, transferring or disposing of it.  |
| 1.1.5 | “Sensitive Personal Data” | information of a sensitive nature relating to, for example, political opinion, religious belief, race or ethnic origin, physical or mental condition of a data subject.   |

### 1.2 Application

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with the eight principles contained within the Act. The second area covered by the Act provides a Data Subject with important rights, including the right to find out what personal information is held by a data controller on electronic and/or paper records.

## 2 REGISTRATION AND NOTIFICATION

The University as a Data Controller is registered on the official register of Data Controllers held by the Information Commission's Office (ICO). It is required to notify the ICO annually of the personal data processing activities that it undertakes. You can inspect the University's registration and notification details at:

<http://www.ico.gov.uk/ESDWebPages/Search.asp?EC=1>

### **3 POLICY STATEMENT**

The University of Ulster is committed to protecting the rights of individuals in accordance with the provisions of the Data Protection Act 1998.

### **4 AIMS OF THE POLICY**

The aims of this Policy are to set out the University's strategy for ensuring compliance with the Act, to ensure that all staff, students or third parties engaged by the University, are aware of their rights and responsibilities under the Act and to minimize the risk to the University of any potential breach of the Act. A breach of the Act could result in damaging valued relationships with stakeholders as well as causing reputational damage to the University and the individual.

This Policy relates to all personal data as defined by the Act held by the University and applies equally to information held in paper and electronic format stored in hard files, on PCs, laptops and other fixed or portable data storage devices. The Policy also applies to photographic material and CCTV footage.

### **5 DATA PROTECTION PRINCIPLES<sup>1</sup>**

The University is committed to the eight Data Protection Principles contained within the Act. These principles represent best standards of practice with respect to the transmission, retention and disposal of personal data. All staff, students and others who process or use any personal data must comply with these Principles. These state that personal data must:

- i) be processed fairly and lawfully;
- ii) be obtained only for the purposes specified and shall only be processed for those purposes;
- iii) be adequate, relevant and not excessive for the purpose for which they are processed;
- iv) be accurate and kept up to date;
- v) be kept for no longer than is necessary;
- vi) be processed in accordance with the rights of data subjects under the 1998 Data Protection Act;
- vii) be protected against unauthorised processing of personal data and against accidental loss or destruction to personal data;
- viii) not be transferred outside the European Economic Area without adequate protection.

### **6 THE DATA PROTECTION CO-ORDINATOR AND DELEGATED OFFICERS**

The University will ensure that it has in place at all times a designated Data Protection Coordinator.

The University's designated Data Protection Coordinator is the Director of Corporate Planning and Governance. The Data Protection Coordinator has the primary responsibility for

---

<sup>1</sup> Summarised from the Data Protection Act 1998 © Crown Copyright 1998

coordinating Data Protection compliance across the University, including notification, and is the ultimate arbitrator within the University in respect of Data Protection matters.

The Data Protection Coordinator has delegated day-to-day responsibility for Data Protection matters to the Head of Governance and Legal Services who is supported by the Policy Officer. These officers are the first point of contact for queries and advice on responsibilities and compliance under the Act; for subject access requests (see section 8); and for liaising with the ICO and other agencies where appropriate. Contact details for these officers are attached at Appendix 1.

## **7 RESPONSIBILITIES OF STAFF AND STUDENTS**

Staff and students at the University are expected to read and understand this Policy and, where required, to seek further clarification from the office of the Data Protection Coordinator. Staff and students are required to abide by this Policy and related policies (see Appendix 2) as from time-to-time amended. Any alleged breaches of the Data Protection Act by staff and/or students will be fully investigated and may result in disciplinary action and may, in some instances, be considered gross misconduct.

All staff and students must apply the criteria listed below as appropriate and relevant at all times to the processing, transmission, retention and disposal of personal data in both electronic and hard copy format.

- i) Ensure that data is kept securely in terms of physical security of offices and filing cabinets with the level of security appropriate to the level of confidentiality and sensitivity of the material.
- ii) Ensure that robust procedures are in place to prevent accidental loss or destruction of personal data.
- iii) Ensure that the use of, and access to, computers, laptops and other portable electronic data processing/storage devices is compliant with University guidance contained within the Code of Practice for Use of University of Ulster Computer Networks, Equipment and Telephone Systems, available at: <http://www.ulster.ac.uk/isd/itus/docs/policies/aucop.htm>
- iv) Staff who have responsibility for supervising students involved in work which requires the processing of personal data are required to ensure that the students are fully aware of the Data Protection Principles and the requirements of this Policy, and the need to obtain the consent of any data subjects involved as appropriate.
- v) Ensure that access to personal data is restricted only to authorised persons.
- vi) Inform University security staff immediately of incidents where persons without proper authorisation are found in areas where personal data is held or processed.
- vii) Ensure that personal information is retained only for the period of time for which it is required. Further information on the length of time records should be kept can be found in the University's Retention and Disposal Schedule available at: <http://www.ulster.ac.uk/isd/archive/schedule/retention.htm>
- viii) Ensure that all personal data is obtained for specified purposes and only processed for those purposes.
- ix) Avoid, in so far as possible, recording personal opinions not based on fact about a Data Subject. These comments will be disclosable.

- x) Ensure that personal information is not disclosed either accidentally or deliberately either verbally or in writing to any unauthorised person or organisation.
- xi) Avoid giving personal data by telephone unless there is a very high degree of certainty that the caller is the person he/she claims to be, and is an appropriate person to receive the data in question.
- xii) Ensure that accurate, up-to-date personal details are provided to the University and notify the University immediately of any changes or errors.
- xiii) There may be circumstances when it is appropriate for the University to share personal information with other organisations, for example if it relates to a criminal investigation. In any such circumstances further guidance should be sought from the Data Protection Coordinator.

The Vice-Chancellor, Pro-Vice-Chancellors, Deans, Heads of School, Research Institute Directors and Directors/Heads of support departments are responsible for having in place appropriate procedures to ensure compliance with the Act within their areas of responsibility. These officers will also be responsible for nominating a suitable representative(s) who will undertake specialist Data Protection training and will work with the Data Protection Coordinator to respond to subject access requests and ensure implementation and dissemination of good practice.

## **8 RIGHTS OF DATA SUBJECTS**

A Data Subject has the right to request access to their personal data held by the University.

Any person who wishes to exercise this right is required to complete a subject access form available upon written request to the Data Protection Coordinator, also available at: <http://plangov.ulster.ac.uk/governance/pdfs/request.doc>.

The University charges a fee of £10.00 to process subject access requests.

If an access request is received by any other member of staff it should be forwarded immediately to the Data Protection Coordinator.

The University undertakes to comply with requests for access to personal information as quickly as possible. In compliance with the law, this will be within 40 calendar days of receipt of a request. However, in exceptional circumstances where a delay is unavoidable, for example, where the University requires further clarification or additional information to enable it to complete the request, the period may be extended provided always that the data subject is informed in writing by the Data Protection Coordinator or their delegated authority of the reason for the delay.

Where an individual requesting information is not known to the University photographic proof of identity may be requested prior to issue of personal data.

## **9 USE OF PERSONAL DATA BY CONSULTANTS OR CONTRACTORS**

Where consultants or contractors are engaged by the University on work that requires the processing of personal data, the University remains the data controller of that data and these organisations will be required to demonstrate that they have arrangements in place to comply with the requirements of the Act and this Policy. In line with the University's Data Protection Policy the Third Party Processing Agreement (the Agreement) should be used when engaging third party suppliers. The Agreement is available at:

[http://plangov.ulster.ac.uk/governance/third\\_party\\_processing\\_agreement.doc](http://plangov.ulster.ac.uk/governance/third_party_processing_agreement.doc)

## **10 COMPLAINTS**

Under Section 42 of the Act an individual has the right to make a complaint if they feel that their personal information has not been handled by the University in accordance with the Data Protection Principles Act. A complaint may be submitted in writing to the Data Protection Coordinator. Alternatively, a complaint may be made to the Office of the Information Commissioner. Full particulars of the Data Protection Act including contact details and the information leaflet 'When and How to Complain' may be found at:

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/data\\_protection\\_-\\_when\\_and\\_how\\_to\\_complain.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_-_when_and_how_to_complain.pdf)

### **POLICY IMPLEMENTATION**

The University will ensure that this Policy and the appropriate procedures are implemented and disseminated and are kept under regular evaluation and review.

### **FURTHER INFORMATION**

Some sources of further information are set out in Appendix 3.

**CONTACTS  
2008/2009**

Data Protection Co-ordinator

Mrs Irene Aston, Director of Corporate Planning  
and Governance

Phone: (028) 7032 4533

e-mail: [ii.aston@ulster.ac.uk](mailto:ii.aston@ulster.ac.uk)

Head of Governance and Legal Services

Mr Eamon Mullan

Phone: (028) 7032 4403

e-mail: [e.mullan@ulster.ac.uk](mailto:e.mullan@ulster.ac.uk)

Policy Officer

Ms Elinor Byrden

Phone: (028) 7032 3354

e-mail: [e.byrden@ulster.ac.uk](mailto:e.byrden@ulster.ac.uk)

**OTHER RELATED UNIVERSITY POLICIES, FORMS and GUIDANCE  
2008/2009**

Code of Practice for Use of University of Ulster Computer Networks, Equipment and Telephone Systems, available at:

<http://www.ulster.ac.uk/isd/itus/docs/policies/aucop.htm>

University of Ulster Retention and Disposal Scheme:

<http://www.ulster.ac.uk/isd/archive/schedule/retention.htm>

Subject Access Request Form:

<http://plangov.ulster.ac.uk/governance/pdfs/request.doc>.

Freedom of Information:

<http://plangov.ulster.ac.uk/governance/freedomofinformation.html>

Student Handbook:

<http://www.ulster.ac.uk/studenthandbook/>

Child Protection Policy:

[http://plangov.ulster.ac.uk/governance/pdfs/child\\_protection\\_policy.pdf](http://plangov.ulster.ac.uk/governance/pdfs/child_protection_policy.pdf)

Equality Scheme:

<http://www.equality.ulster.ac.uk/pdf/uuequalityscheme.pdf>

Disability Disclosure Guidelines:

[http://www.equality.ulster.ac.uk/2412-disclosure\\_guidelines.pdf](http://www.equality.ulster.ac.uk/2412-disclosure_guidelines.pdf)

Special Educational Needs and Disability (NI) Order 2005 - Guidance

[http://www.equality.ulster.ac.uk/1587-sendo\\_booklet.pdf](http://www.equality.ulster.ac.uk/1587-sendo_booklet.pdf)

**FURTHER RELEVANT INFORMATION IS AVAILABLE AT:**

Data Protection Act 1998, legislation in full at:

[http://www.opsi.gov.uk/acts/acts1998/ukpga\\_19980029\\_en\\_1](http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1)

Higher Education Statistics Agency:

<http://www.hesa.ac.uk/dataprot/>

Information Commissioner's website:

<http://www.ico.gov.uk/>

Joint Information Systems Committee (JISC) Legal Information Service:

<http://www.jisclegal.ac.uk/dataprotection/dataprotection.htm>

Joint Information Systems Committee (JISC) Data Protection Code of Practice for the HE & FE Sectors

[http://www.jisc.ac.uk/publications/publications/pub\\_dpacop\\_0101.aspx](http://www.jisc.ac.uk/publications/publications/pub_dpacop_0101.aspx)