QUEEN'S UNIVERSITY BELFAST

DATA PROTECTION POLICY

Introduction

Queen's University Belfast is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998 ("the Act"). This document is the University's policy in response to the requirements of the Act.

Purpose and Scope

In carrying out its responsibilities, the University will be required to process certain information about individuals such as staff, students, graduates and other users, defined as "**data subjects**" in the Act. This information, or "**data**" as it is often referred to, must be processed according to the Data Protection Principles contained within the Act.

Queen's University staff and students, or others who process or use any personal information on behalf of the University (i.e. "**data users**"), have a personal responsibility to ensure that they adhere to the University's Data Protection Policy and the Act.

Any breach of this Policy, or the Act, by a member of staff or student, can be considered as a disciplinary matter. It may also be a criminal matter for which the University, and the individual concerned, could be held criminally liable.

Data Protection Principles

Queen's University data users must comply with the eight Data Protection Principles. These define how data can be legally processed. "**Processing**" includes obtaining, recording, holding or storing information and using it in any way.

Personal data must:

1. Be processed fairly and lawfully and only when certain conditions are met.
2. Only be obtained and processed for specified and lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and, where necessary, up to date.
5. Be kept for no longer than necessary.
6. Be processed in accordance with data subjects' rights.
7. Be protected by appropriate security measures.
8. Not be transferred outside the European Economic Area, to countries without adequate protection unless the consent of the data subject has been obtained.

The Act defines both **personal data** and **sensitive personal data** (please refer to the Definitions section on Page 6). Data users must ensure that the necessary conditions are satisfied for the processing of personal data. In addition, they must adhere to the extra, more stringent conditions in place for the processing of sensitive personal data. Sensitive personal data should normally only be processed if the data subjects have given their explicit (written) consent to this processing, and must

be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file.

Security

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 and procedures contained within this policy, staff and students are also advised to read and adhere to the University's Information Security Policy, available at:

http://www.qub.ac.uk/directorates/InformationServices/Services/Security/

Responsibilities - General Principles

All personal data held on behalf of the University, whether electronically or on paper, must be kept securely, no matter whether it is kept by an individual, Faculty, School or Professional Services Directorate. Personal data must not be disclosed to any unauthorised third party by any means, accidentally or otherwise.

Where staff are unsure as to whether they can legitimately share/disclose personal data with other individuals, either within or outside the University, they **must** seek advice from their line manager. Further guidance is also available from the Information Compliance Unit, on request.

All staff should note that unauthorised disclosure may be a disciplinary matter. It may also be a criminal matter for which the University and the individual concerned could be held criminally liable.

Faculty/School/Directorate Responsibilities

Senior Management within Faculties, Schools and Directorates have responsibility for ensuring that:

- All staff are aware of their responsibilities under the Data Protection Policy and the Act and of the risks/consequences of failure to comply with the related requirements.
- All staff complete the mandatory on-line training programme.
- That mechanisms are put in place to protect data (and particularly sensitive data) during day-to-day operations. This will include, but not exclusively, guidance supporting the password protection of documents; photocopiers; mail; secure filing etc.
- All personal data being processed within the Faculty/School/Directorate complies with the Data Protection Policy (including any subsequent amendments or additions) and with the Act.
- That all forms and correspondence used by the Faculty/School/Directorate, to request personal data, clearly state the purposes for which the information is to be used, the period of time it is to retained, and to whom it is likely to be disclosed.
- All personal data held within the Faculty/School/Directorate is kept securely and is disposed of in a safe and secure manner when no longer needed.
- All Data Protection breaches are notified to the Information Compliance Unit, with remedial action taken to mitigate the risk of reoccurrence.
- An annual audit of the personal data within the Faculty/School/Directorate is carried out and recorded.
- Where a new or different purpose for processing data is introduced, the Information Compliance Unit is advised accordingly.
- All contractors, agents and other non-permanent University staff used by the Faculty/School/Directorate are aware of, and comply with, the Data Protection Policy and the Act.

Staff Responsibilities

All staff must take personal responsibility for ensuring that:

- They are aware of their responsibilities under the Data Protection Policy and the Act and the risks/consequences of failure to comply with the related requirements. Where they are uncertain of their responsibilities, they must raise this with their line manager.
- They complete the mandatory on-line training programme.
- Personal data relating to any living individual (staff, students, contractors, members of the public etc.) which they hold or process is kept securely.
- Personal data relating to any living individual is not disclosed, either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- All Data Protection breaches are notified to their line manager, with remedial actions implemented to mitigate the risk of reoccurrence.
- When supervising students who are processing personal data, that they are aware of the Data Protection Principles and the University's Data Protection Policy.
- 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;

Student Responsibilities

All students must take personal responsibility for ensuring that:

- When using University's facilities to process personal data (for example, in course work or research), they seek advice from their Supervisor/Advisor of Studies on their responsibilities under the Act.
- 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;

Information Compliance Unit Responsibilities

The Information Compliance Unit must ensure that:

- The University's Data Protection Policy is regularly reviewed and updated in line with best practice.
- Staff have access to training on their responsibilities under the Data Protection Policy and the Act, both on-line and through more traditional training methods.
- Responses to requests for information under the Act, and related compliance matters, are dealt with in a timely manner and in line with the requirements of the Act.
- Advice and guidance on any area of the Policy or the Act is provided to staff and students, on request.

Notification

Every year, the University, as a Data Controller and Data Processor, is required to provide the Information Commissioner's Office (ICO) with a comprehensive report, detailing the following:

(i) The personal data that it will process.
(ii) The categories of data subject to which personal data relates.
(iii) The purposes for which the personal data will be processed.
(iv) Those people to whom the University may wish to disclose the data.
(v) Any countries or territories outside the European Economic Area to which the University may wish to transfer personal data.
(vi) A general description of security measures taken to protect personal data.

When processing for a new, or different, purpose is introduced, the individuals affected by that change will be informed and the University's official notification to the ICO updated accordingly.

Upon request, the University is also required to provide staff, students and other relevant data subjects with details on the personal data held by the University about them, and the reasons for which it is held/processed. Such requests are handled by the University's Information Compliance Unit, located in the Registrar's Office, Lanyon South.

Disposal Policy for Personal Data

The Act places an obligation on the University to exercise care in the disposal of personal data, including protecting its security and confidentiality during storage, transportation, handling, and destruction.

All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved, how sensitive it is, and the format in which it is held.

Retention Policy for Personal Data Records

The Act places an obligation on the University not to hold personal data for longer than is necessary. The ICO (www.ico.gov.uk) provides general guidance on the retention of personal data.

Contractors, Short-Term and Voluntary Staff

The University is responsible for the use made of personal data by anyone working on its behalf, whether as an agent, in a voluntary capacity, or as a consultant or contractor undertaking work for the University. Additional guidance in this area is available from the Information Compliance Unit on request.

Transfer of Data Outside the University

When the University shares personal data with another organisation, liability for adherence to the Act, in relation to this data, rests with the University. Should that organisation breach the Act, the University would be held responsible for that breach.

If a Faculty/School/Directorate must share personal data with other organisations in order to conduct business, a data sharing agreement may be required. Information and guidance on drafting Data Sharing Agreements is available from the Information Compliance Unit on request.

Transfer of Data Overseas

The Eighth Data Protection Principle prohibits the transfer of personal data to any country outside the European Economic Area (EEA) (EU Member States, Iceland, Liechtenstein and Norway) unless that country ensures an adequate level of protection for data subjects.

In all instances where personal data is being sent outside the EEA, the consent of the data subject should be obtained before their personal information is sent. This includes requests for personal data including from overseas colleges, financial sponsors and foreign governments. Information and guidance on the transfer of data overseas is available from the Information Compliance Unit, on request.

Use of CCTV

The University's use of CCTV is governed by a Code of Practice, issued by the ICO:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

For reasons of crime prevention and security, a network of surveillance cameras, including body worn cameras, are in operation throughout campus. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out by a limited number of specified staff;
- The recordings will be accessed only by authorised personnel;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

Related Policies

This policy should be read in conjunction with:

- Freedom of Information Policy;
- Information Security Policy;
- Computer Resources – Regulations for Acceptable Use;
- Information Handling Policy;
- Password Policy;
- Data Security Guidance;
- Surveillance Camera Policy;
- Records Management Strategy.

Making a Request

Staff, students, users of the University's facilities, and members of the public have the right to access personal data that is being kept about them insofar as it falls within the scope of the Act. Requests should be made in writing via email to info.compliance@qub.ac.uk or via post to:

Information Compliance Unit
Registrar's Office
Queen's University Belfast
BT7 1NN

The University reserves the right to charge an administrative fee of £10 on each occasion that access is requested and will seek to ensure that the information is provided within 40 calendar days.

There is no right to an internal review of a decision taken regarding release of personal information under the Data Protection Act 1998. If the requestor is not satisfied with the response received from the University they do, however, have the right to appeal directly to the ICO.

Further Information

Further information on this policy is available from the Registrar's Office on request. Full contact details are provided above.

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.
Sensitive Personal Data	Personal data consisting of information as to race/ethnic origin; political opinion; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; and criminal record.
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 Queen's University Belfast. This includes university staff who collect and process data on behalf of the University, and students who are collecting and processing personal data 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.
Data Users	Refers to both Data Controller and Data Processors.

October 2016