

QUEEN'S UNIVERSITY BELFAST

DATA PROTECTION POLICY

Policy Statement

Queen's University Belfast is required by law to comply with the Data Protection Act 1998 (1998 Act). This document is the University's policy in response to the requirements of the 1998 Act.

The University is committed to ensuring that all employees, registered students, agents, contractors and data processors comply with the 1998 Act, regarding the processing and confidentiality of any personal data held by the University. To do this Queen's University must comply with the Data Protection Principles contained within the 1998 Act.

Data Protection Principles

Personal data shall:

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.

Queen's University staff and students, or others who process or use any personal information on behalf of the University, must ensure that they follow these principles at all times.

All staff and students have an individual responsibility to ensure that they adhere to the University's Data Protection Policy and the 1998 Act.

Any breach of the University's Data Protection Policy or the 1998 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.

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

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 personal 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
Recipient	Any person or organisation to whom personal data are disclosed.

Notification

The University will register as a Data Controller and a Data Processor and will notify the Information Commissioner of:-

- (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 information.
- (v) Any countries or territories outside the European Economic Area to which the University may wish to transfer the personal data.
- (vi) A general description of security measures taken to protect the data.

Upon request, the University shall notify all staff, students and other relevant data subjects of the types of personal data held by the University about them, and the reasons for which it is processed.

The information currently held by the University, and the purposes for which it is processed, form the official notification that has been submitted to the Information Commissioner's Office. When processing for a new or different purpose is introduced the individuals affected by that change will be informed and the official notification will be amended.

Further details can be obtained from the University's Data Protection Co-ordinator.

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 section of the policy, staff and students are also advised to read and adhere to the University's Information Security Policy.

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, School or the University Administration and Support Directorates. Personal data must not be disclosed to any unauthorised third party by any

means, accidentally or otherwise. Staff are reminded that it is the individual's responsibility to adhere to this policy document. It is University policy that unauthorised disclosure may be viewed as a valid reason for disciplinary action.

Responsibilities

School / Department Responsibilities

Key post holders have responsibility for ensuring that:

- All personal data being processed within the School/Directorate/Unit complies with the Data Protection Act 1998 and the University's Data Protection Policy (including any subsequent amendments or additions) and is included in the University's official Data Protection Notification.
- An annual audit of the personal data within the School/Directorate/Unit is carried out and recorded.
- That all forms and correspondence used by the School/Directorate/Unit to request personal data, clearly state the purposes for which the information is to be used, the period of time it is to be retained, and to whom it is likely to be disclosed.
- All contractors, agents and other non-permanent university staff used by the school /department are aware of and comply with, the Data Protection Act 1998 and the University's Data Protection Policy.
- All personal data held within the School/Directorate/Unit is kept securely and is disposed off 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. Unauthorised disclosure may be considered a disciplinary matter.
- When supervising students who are processing personal data that they are aware of the Data Protection Principles 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 staff supervisor / advisor in the relevant department / faculty, who will provide further information about the university's policy on data protection compliance.

The University shall not be held responsible for errors of which it has not been informed.

Disposal Policy for Personal Data

The Data Protection Act 1998 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 is it?), and the format in which it is held.

Retention Policy for Personal Data Records

The Data Protection Act 1998 places an obligation on the University not to hold personal data for longer than is necessary. The Information Commissioner's Office at www.ico.gov.uk provides general guidance on retention of personal data.

Processing Personal Data

Staff should ensure that they are familiar with the University's Data Protection Policy and official Data Protection Notification.

Staff whose work involves the processing of personal data must ensure they observe the eight data protection principles of the 1998 Act and comply with the University's Data Protection policy and any amendments or supplementary guidance issued from time to time.

Staff whose work includes responsibility for supervision of students' academic work have a duty to ensure that students observe the eight principles of the 1998 Act and comply with the University's Data Protection policy and any amendments or supplementary guidance issued from time to time. All staff should ensure that any holding or processing of personal data is included in the University's official data protection notification.

All staff and students are responsible for ensuring that:

- Any personal data, which they hold or use, in whatever format, is kept securely and that appropriate care is taken in disposing of personal data.
- Personal data is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Disclosure of Personal Data

Staff who are unsure as to the nature of authorised third parties, to whom they can legitimately disclose personal data, should check the University's official data protection notification and if still in doubt seek advice from their line manager or the Data Protection Co-ordinator.

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

Sensitive Personal Data

The 1998 Act introduces a new category of sensitive personal data, which is subject to additional safeguards.

Sensitive personal data is any personal data, which includes information on

- racial or ethnic origin,
- 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 (written) consent to this processing.

(Explicit consent, is consent that refers to specific and identifiable processing of personal data,. Such consent should where possible be obtained in writing as this can be used for future reference, whilst explicit verbal consent cannot)

If this is not possible, the data may still be processed if one of a number of other conditions is met. The University, may process sensitive personal data without the subjects' explicit consent if the processing is necessary:

- Because of any right or obligation imposed by employment law.
- For medical purposes, including medical research, and is undertaken by a health professional or equivalent person.
- With appropriate safeguards, for equal opportunities monitoring of information on ethnic origin.

Disclosure of such information without consent is permitted only in "life or death" circumstances, e.g., if a data subject is unconscious, a tutor can tell medical staff that the data subject has a medical condition.

Sensitive personal data 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.

Incoming and Internal Mail

The following principles should be applied to the processing of incoming and internal mail:

- Paper-based mail that is marked 'Personal', or 'Private and Confidential', or which appears to be of a personal nature, should only be opened by the addressee, or a designated person. Unless paper-based mail items are marked in this way, it will be assumed that they do not contain personal or confidential information.
- Any other mail will be assumed not to contain confidential information, as designated by the 1998 Act.
- Staff should not use their University address for non-University matters.

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, or in a voluntary capacity, or as a consultant or contractor undertaking work for the University. Anyone in this position must:

- Ensure that any personal data collected or processed in the course of work undertaken for the University, is kept securely and confidentially. This applies whether the data is an integral part of the work, or whether it is simply contained on media or in places which contractors etc need to access; it applies whether or not the University explicitly mentions the data in the contract.
- Ensure that all such data is returned to the University on completion of the work, including any copies that may have been made.
- Give the University details of any processing of personal data that will be undertaken as part of a contract, so that the University can ensure that the appropriate data protection notification is made, and ensure that neither they nor their employees nor any sub-contractors carry out any processing other than that which has been agreed.
- Give the University details of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor. The University will need to satisfy itself that such disclosures are covered by its data protection notification, and they should not be made until the written consent of the University has been received. Where such disclosures are not covered by the notification, the University will advise the contractor or other worker not to undertake disclosure until consent is received from the data subjects concerned.

- Ensure that any personal data made available by the University, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the University.
- Take all practical and reasonable steps to ensure that they, their employees, or any sub-contractors do not seek to obtain access to any personal data beyond what is essential for the work to be carried out properly.

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.