QUEEN'S UNIVERSITY BELFAST

DATA PROTECTION POLICY

1. Introduction

1.1 Queen's University Belfast is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This document is the University's policy in response to the requirements of the GDPR.

2. Purpose and Scope

2.1 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 GDPR.

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

2.3 Any breach of this Policy, or the GDPR, 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.

2.4 The GDPR defines both **personal data** and **special category personal data** (please refer Appendix 1, Definitions). 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 special category data.

2.5 Special Category Personal Data should only be processed if meets one of the conditions for processing detailed in Appendix 2 of this policy. It is recommended that special category records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file.

3. Data Protection Principles

3.1 Queen's University staff and students, or others who process or use any personal information on behalf of the University, must comply with the six 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.

3.2 Personal data must:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which those data are processed; and
- Processed in a manner that ensures appropriate security of the personal data.

3.3 Accountability is central to the GDPR. As a data controller the University is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator (the Information Commissioner).

4. Lawful basis for processing

4.1 The University will identify the lawful basis for processing personal data.

4.2 The lawful basis for processing are set out in Article 6, GDPR and at least one of these conditions must apply whenever the University processes personal data.

Consent: the individual has given clear consent to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract which you have with the individual, or because they have asked you take specific steps before entering into a contract.

Legal obligation: the processing is necessary for the University to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary to perform a task in the public interest or official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests of the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply where the University is processing data to perform official tasks).

The University will provide information to data subjects about the lawful basis (or bases) for processing within a privacy notice.

5. Rights of data subjects

5.1 Data subjects are afforded a number of rights under the GDPR. These are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automate decision making and profiling.

5.2 **The right to be informed**

The University will inform data subjects, typically through a privacy notice, how personal data held by the University, whether obtained directly or not, is processed.

The information the University will supply about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

5.3 **The right of access**

Under GDPR, data subjects will have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data; and

- Other supplementary information (this largely corresponds with information provided in the privacy notice).

The University will provide a copy of the information free of charge. A "reasonable fee" may be required or a request may be refused where it is manifestly unfound or excessive, particularly if repetitive.

If a request is refused an explanation as to why will be provided and the data subject will be informed of their right to complain to the Information Commissioner.

The identity of a data subject may be verified before release through the provision of relevant identification documents.

Where possible and proportionate the University will provide the data requested in the preferred format of the applicant.

Whilst data subjects have the general right of access to their own personal information which is held, the University will be mindful of those circumstances where an exemption may apply and, in particular, the data protection rights of third parties who may also be identifiable from the data being requested.

Requests to access personal data can be made via email to info.compliance@qub.ac.uk and will be responded to within one month.

5.4 The right to rectification

The University will rectify personal data where it is inaccurate or incomplete.

Where the University has disclosed the personal data in question to others, each recipient will be contacted and informed of rectification unless this is impossible or involves disproportionate effort.

A request for rectification can be made via email to info.compliance@qub.ac.uk and will be responded to within one month. Where a request is particularly complex the University may request an extension, up to an additional two months.

Where the University cannot take action to rectify an explanation will be provided to the data subject and they will be informed of their right to complain to the Information Commissioner and to judicial remedy.

5.5 The right to erasure – also known as "the right to be forgotten"

Where there is no compelling reasons for the continued processing of an individual's personal data the University will delete or remove the personal data at the request of the data subject.

Data may be erased to prevent processing in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed:
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

(Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger).

A request for erasure may be refused where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

If the personal data in question has been disclosed to others, we will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort.

Upon request the University will inform the individual about these recipients.

5.6 **Right to restrict processing**

The University will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we will restrict the processing until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the data subject requires the data to establish, exercise or defend a legal claim.

Where the personal data in question has been disclosed to others, we will contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the University will also inform the data subject about these recipients.

The University will inform the data subject if it is decided to lift a restriction on processing.

5.7 **Right to data portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services and allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

• to personal data an individual has provided to a controller;
• where the processing is based on the individual's consent or for the performance of a contract; and
• when processing is carried out by automated means.

Where the data requested meets these requirements the University will provide the personal data in a structured, commonly used and machine readable form and free of charge.

If the data subject requests it, the University will transmit the data directly to another organisation, if this is technically feasible.

The University will respond without undue delay, and within one month. This can be extended by two months where the request is complex or we have received a number of requests.

5.8 Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

The University will stop processing the personal data unless:
• There is compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
• the processing is for the establishment, exercise or defence of legal claims.

Where appropriate the University will inform individuals of their right to object "at the point of first communication" and in our privacy notice. This will be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

The University will stop processing personal data for direct marketing purposes as soon as we receive an objection.

Where the University is conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

5.9 Rights related to automated decision making including profiling

The University will carry out processing under Article 22(1) of the GDPR where the University is authorised or required to do so and it is the most appropriate way to achieve the aims of processing.

Where a data subject wishes to have an automated decision reconsidered they may submit a request via email to info.compliance@qub.ac.uk

6. Security

6.1 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/

7. Responsibilities - General Principles

7.1 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 Directorates. Personal data must not be disclosed to any unauthorised third party by any means, accidentally or otherwise.

7.2 Where staff are unsure as to the 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.

7.3 **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.**

7.4 ***Faculty/School/Directorate Responsibilities***

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

- All staff are aware of their responsibilities in this area, and the risks of failure to comply with the Data Protection Policy and the Act.
- All staff complete the mandatory on-line training programme.
- All Data Protection breaches are notified to the Information Compliance Unit, with remedial action taken to mitigate the risk of reoccurrence.
- 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 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.
- 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 Act and the University's Data Protection Policy.

7.5 ***Staff Responsibilities***

All staff must take personal responsibility for ensuring that:

- They are aware of their responsibilities in this area, and the risks of failure to comply with the Data Protection Policy and the Act. Where they are uncertain of their responsibilities, they refer this to 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;

7.6 ***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;

7.7 **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 Policy, the GDPR and the Data Protection Act 2018, both on-line and through more traditional training methods.
- Responses to requests for information and related compliance matters are dealt with in a timely manner and in line with the requirements of data protection legislation.
- Advice on any area of the policy or data protection legislation is provided to staff and students, on request.

8. Notification

8.1 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:

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

8.2 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.

8.3 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.

9. Disposal Policy for Personal Data

9.1 The GDPR 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.

9.2 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.

10. Retention Policy for Personal Data Records

10.1 The GDPR places an obligation on the University not to hold personal data for longer than is necessary. The ICO (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/) provides general guidance on the retention of personal data.

11. Contractors, Short-Term and Voluntary Staff

11.1 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.

12. Transfer of Data Outside the University

12.1 When the University shares personal data with another organisation the University must insure that the organisation has in place the requisite controls and security to demonstrate compliance with the GDPR.

12.2 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.

13. Transfer of Data Overseas

13.1 GDPR 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.

13.2 Information and guidance on the transfer of data overseas is available from the Information Compliance Unit on request.

14. Use of CCTV

14.1 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

14.2 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.

15. Related Policies

15.1 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.

Appendix 1

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 relating to natural (living) persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
Special Category 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; sexual orientation; genetics and biometrics (where used for ID purposes).
Criminal offence data	Personal data relating to criminal convictions and offences, or related security measures.
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

Appendix 2

Conditions for processing special category data

The conditions are listed in Article 9(2) of the GDPR:

1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

2. The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4. The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

5. The processing relates to personal data which are manifestly made public by the data subject;

6. The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

7. The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

8. The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

9. The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

•Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (h), (i) and (j).

•Schedule 1 Part 2 contains specific ‘substantial public interest’ conditions for Article 9(2)(g).

•In some cases you must also have an ‘appropriate policy document’ in place to rely on these conditions.