

Queen's Accommodation

Accommodation Data Protection Policy and Procedure

1 Introduction

- 1.1 Queen's Accommodation is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.
- 1.2 The University holds personal information about individuals such as employees, students, graduates and others, defined as data subjects in the Act.

2 Principles

- 2.1 To comply with the law, information 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 Data Protection Principles, which are set out in the Data Protection Act 1998 and ensure the future proofing of all procedures in line with the General Data Protection Regulation (GDPR) which applies in the UK from 25 May 2018.
- 2.2 The Data Protection Principles state that personal data shall:
 - i. Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
 - ii. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
 - iii. Be adequate, relevant and not excessive for those purposes.
 - iv. Be accurate and kept up-to-date.
 - v. Not be kept for longer than is necessary for that purpose.
 - vi. Be processed in accordance with the data subject's rights.
 - vii. Be kept safe from unauthorised access, accidental loss or destruction.
 - viii. Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

2.3 What is Personal Data?

2.3.1 Definition

Any information 'about' a person, or from which a person can be identified, even indirectly.

2.3.2 Personal Data

- i. The GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data, HR records, customer lists, or contact details etc., the change to the definition should make little practical difference.
- ii. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.
- iii. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

2.3.3 Sensitive Personal Data

- i. The GDPR refers to sensitive personal data as “special categories of personal data”.
- ii. The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- iii. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.
- iv. Personal data has a broad ranging definition and can include not only items such as home and work address, age, telephone number and schools attended but also photographs and other images. Sensitive personal data consists of racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and criminal record.
- v. Photographs and videos (where the person can be easily identified)
- vi. Expressions of opinion
- vii. Data processed by computer or internet software, held in emails or on a mobile device
- viii. Data recorded and processed manually as part of a filing system, paperwork and even handwritten notes.

3 Policy

- 3.1 Queen's Accommodation complies with the Data Protection Act 1998 and Queen's University Data Protection Policy safeguarding students' personal data from being released to third parties, except where it is a legal requirement to do so or where students have given their consent.
- 3.2 When communicating with students, staff must be mindful that personal data, including mobile phone numbers, are not compromised.
- 3.3 Any breach of the policy may result in the University, as the registered Data Controller, being liable in law for the consequences of the breach. This liability may extend to the individual processing the data and his/her Head of Department under certain circumstances.

4 Staff Responsibilities

- 4.1 Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy.

4.1.1 Senior Management must ensure that:

- i. All staff are aware of their responsibilities under the Data Protection Act 1998
- ii. All staff complete the mandatory online training programme
- iii. Mechanisms are put in place to protect data during day-to-day operations
- iv. All personal data being processed complies with the Policy and the Act
- v. All personal data is kept securely and is disposed of in a secure manner when no longer needed
- vi. All Data Protection breaches are notified to the Information Compliance Unit (ICU), with remedial action taken to mitigate the risk of reoccurrence.

4.1.2 Staff members must ensure that:

- i. Personal data is processed in accordance with the Data Protection Act 1998 and the University's Data Protection Policy
- ii. All personal data is kept securely
- iii. When supervising students who are processing personal data, that those students are aware of the Data Protection Principles, and the University's Data Protection Policy
- iv. No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- v. Personal data is kept in accordance with the University's retention schedule
- vi. Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance Unit (ICU)
- vii. Any data protection breaches are swiftly brought to the attention of the ICU and that they support the ICU in resolving breaches
- viii. Where there is uncertainty around a Data Protection matter, advice is sought from the ICU.

- 4.1.3 This Policy may be implemented when dealing with student related issues including disciplinary, residential fee payments and accommodation.

5 Student Responsibilities

5.1 Students are responsible for:

- i. Familiarising themselves with the Data Protection Policy provided when they register with the University
- ii. Ensuring that their personal data provided to the University is accurate and up-to-date.

6 Procedure

- 6.1 Queen's University have appointed a Data Protection Officer to handle day-to-day issues which arise, and to provide members of the University with guidance on Data Protection issues to ensure they are aware of their obligations.
- 6.2 When personal data is transferred internally the recipient must only process the data in a manner consistent with the University's original purpose for which the data was collected.
- 6.3 Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member. Staff members must:
 - i. Protect personal data sent by email
 - ii. Use the correct and most up-to-date email address
 - iii. Turn off the 'auto-correct' feature in Outlook when they are processing personal data
 - iv. Use the BCC (blind copy) function unless they are certain that recipients need to know who the other recipients are
 - v. Double-check that they have added the correct attachment before sending an email
 - vi. Contact the recipients separately to provide the password if sending a password-protected document
 - vii. Ensure that the content is accurate and that the language and tone of the email is professional and appropriate.
- 6.4 Staff members must protect personal data held electronically:
 - i. Ensure any documents containing personal data are password-protected
 - ii. Save personal data in secure areas i.e. secure network drives
 - iii. Lock their computer screen any time you leave their desk
 - iv. Change their password regularly and do not share passwords with colleagues
 - v. Use secure photocopiers/printers when working with personal data
 - vi. Angle computer screens so that people walking past cannot view the detail displayed on them
 - vii. Submit a written application to the QUB Security Section Leader in the event CCTV footage pertaining to a specific date and time range is required, completing the necessary authorisation documentation
 - viii. Information to consider when staff are collecting photographic images: what is the image being used for, how it will be displayed/used, how long it will be kept, who will be able to view it and who the data subject should contact if they wish to withdraw their consent.

6.5 Staff members must protect personal data during telephone conversations:

- i. Ask the individual where possible, to submit their request in writing via their organisation's email system or company headed paper
- ii. Do not identify the person clearly

6.6 Requests for information about any living individual should not normally be given without the explicit written consent of that individual. If in doubt, please contact the Information Compliance Unit for advice.

6.7 Staff members must protect personal data sent in the post:

- i. Ensure that the address is correct and up-to-date
- ii. Send documents to a named person if possible – not a department or team
- iii. Always put a covering letter marked 'Strictly Private and Confidential' with your contact details in the envelope with the information
- iv. Seal the envelope securely and mark it 'Private and Confidential'
- v. Write your return address on the back of the envelope
- vi. Ensure mail that is marked 'Personal' or 'Private and Confidential', or which appears to be of a personal nature, is opened by the addressee, or a designated person.

7 Use of Electronic Devices to Capture Photographic Evidence

7.1 Photographs of living people are personal data and therefore fall under the Data Protection Act 1998 and must be treated accordingly.

7.2 Sensitive personal data consists of information on someone's racial or ethnic origin, political opinions, religious beliefs, trade union activity, physical or mental health, sexual life or any offences committed. Photographs can often contain some of this information, so in certain circumstances, photographs can be sensitive personal data.

7.3 Photographs of crowds are not classified as personal data, providing no one person is the focus of the photograph. It is good practice, before taking a photograph of a group, to verbally ask permission to do so, therefore giving anyone who does not wish to be included the opportunity to opt out. Crowd photographs which are cropped to focus on one individual will become subject to the Act.

7.4 Photographs taken purely for personal use are exempt from the Data Protection Act, e.g. photographs taken by family members at graduation.

7.5 Photographs taken at registration are only to be used for security purposes and access to services and can only be used for those reasons. If you wish to use registration photographs for any other reason, you should obtain consent from the individual.

7.6 Staff or student photographs should not be displayed on the wall (noticeboards etc.) or online without consent from the individuals concerned. Any staff or students who do not wish for their photograph to be displayed in a public area should not be forced to do so.

8 Police Requests

8.1 All PSNI requests for personal data must be made known to your Line Manager and immediately forwarded to the Information and Compliance Unit. The Unit will take responsibility for issuing the University's response to the PSNI. PSNI must present the completed

9 Processing Sensitive Information

9.1 Sometimes it is necessary to process information about a person's criminal convictions, race and gender and family details. This may be to ensure the University is a safe place for everyone, or to operate other University policies, such as the Sick Pay Policy or Equal Opportunities Policy. The University will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes or disabilities. The University will only use the information in the protection of the health and safety of the individual, but will need consent to process for example, in the event of a medical emergency. As this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals. Staff and students will be asked to give express consent for the University to do this.

10 Contact Information

10.1 For further information and guidance, please contact the Information and Compliance Unit:

Email: info.compliance@qub.ac.uk

Telephone: 028 90 97 2505 / 2506

11 General Data Protection Regulation (GDPR)




11.1 The GDPR applies to 'controllers' and 'processors'.

11.2 Processor - required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

- 11.3 Controller - not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- 11.4 The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- 11.5 Consent
- i. The GDPR has references to both ‘consent’ and ‘explicit consent’. Consent under the GDPR requires some form of clear affirmative action. Consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time.
- 11.6 Principles
- i. Under the GDPR, the data protection principles set out the main responsibilities for organisations.
 - ii. The principles are similar to those in the DPA, with added detail at certain points and a new accountability requirement. The GDPR does not have principles relating to individuals’ rights or overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter III and Chapter V respectively).
 - iii. The most significant addition is the accountability principle. The GDPR requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity. This is explained in greater detail later in this guide.
- 11.7 Article 5 of the GDPR requires that personal data shall be:
- i. processed lawfully, fairly and in a transparent manner in relation to individuals;
 - ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - iv. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - v. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

- purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
 - vi. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- 11.8 Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.
- 11.9 The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.
- 11.10 The GDPR provides the following rights for individuals:
 - i. The right to be informed
 - ii. The right of access
 - iii. The right to rectification
 - iv. The right to erasure
 - v. The right to restrict processing
 - vi. The right to data portability
 - vii. The right to object
 - viii. Rights in relation to automated decision making and profiling.
 - ix. This part of the overview explains these rights.
- 11.11 The right to be informed encompasses your obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how you use personal data.
- 11.12 What information must be supplied?
 - 11.12.1 The GDPR sets out the information that you should supply and when individuals should be informed.
 - 11.12.2 The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.
 - 11.12.3 Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide.
 - 11.12.4 The information you supply about the processing of personal data must be:
 - i. concise, transparent, intelligible and easily accessible;
 - ii. written in clear and plain language, particularly if addressed to a child; and
 - iii. free of charge.
- 11.13 The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer		
Purpose of the processing and the legal basis for the processing		
The legitimate interests of the controller or third party, where applicable		
Categories of personal data		
Any recipient or categories of recipients of the personal data		
Details of transfers to third country and safeguards		
Retention period or criteria used to determine the retention period		
The existence of each of data subject's rights		
The right to withdraw consent at any time, where relevant		
The right to lodge a complaint with a supervisory authority		
The source the personal data originates from and whether it came from publicly accessible sources		

Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data		
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.		
When should information be provided?	At the time the data are obtained.	<p>Within a reasonable period of having obtained the data (within one month)</p> <p>If the data are used to communicate with the individual, at the latest, when the first communication takes place; or</p> <p>If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.</p>

Date of Assessment:	Policy Review Date:
Assessor: Mike Uprichard	Sept 2023