



QUEEN'S
UNIVERSITY
BELFAST

A GUIDE TO HANDLING PERSONAL AND SENSITIVE DATA

STUDENTS, CLUBS
AND SOCIETIES



Students, Clubs and Societies

The General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 were brought into effect on the 25th May 2018, with the purpose of protecting personal and sensitive data and ensuring transparency in how this data is used.

How the University uses your data, to provide your educational and student experience services, can be viewed at the University's Privacy Notice webpage www.qub.ac.uk/privacynotice

We all have a role to play in protecting our fellow students' data and we can all help to protect each other and ourselves from potential data privacy incidents.

What is Personal Data?

Personal Data can be categorised as: Information relating to an identified or identifiable natural person (data subject), directly or indirectly. This could be through a reference number, a name, location data, online identifier, or to one or more factors specific to the physical, physiological, cultural or social identity of that natural person.

Things like: Names, addresses, emails, phone numbers, personal ID numbers, photographs and online identifiers (such as IP addresses).

There is also a category specifically for 'sensitive' personal data or 'special categories' of personal data as the legislation calls it.

These would be:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

These information types are protected under the new legislation and we must have a clear lawful basis for capturing, processing and storing this information.

Clubs and Societies

It could easily be forgotten that when you are running or managing a sports or social club, that you will be responsible for the handling of personal and possibly sensitive personal data. You will have the responsibility for ensuring that this data is kept secure and confidential. You will also be responsible for ensuring that only the data that is required is collected and the data is only retained for the duration that it is required.



Questions you should be asking about the data you currently hold and/or want to collect:

- What data do I require for the purposes of fulfilling our club/society administrative needs?
- Is this data personal and sensitive in nature?
- How long are we required to hold this data for the purposes of fulfilling our club/society function?
- How will the data be deleted?
- Where and how will we collect the data?
- Where and how will the data be stored?
- Are we required to share the data with any other affiliates or third parties?
- Are we being transparent? (ie. Do we need to create a privacy notices for our members?)

If you need assistance answering these questions or to help produce a privacy notice, please contact us on info.compliance@qub.ac.uk

Accountability

The Accountability principle requires evidence of data protection compliance in the form of appropriate documentation. Data Privacy Impact Assessments, Retention Schedules and Information Asset Registers are examples of records that the Information Commissioner's Office will expect to see if required to investigate a personal data breach.

For assistance with this documentation, please contact the Information Compliance Unit info.compliance@qub.ac.uk