QUEEN'S UNIVERSITY BELFAST

A GUIDE TO HANDLING PERSONAL AND SENSITIVE DATA

STAFF

Protecting Personal Data

Data Protection is the fair and proper use of information about people. The following sets out some practical steps to protect the personal data we process and support compliance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Data Protection legislation puts a focus on the personal responsibilities of each individual employee. We all have a part to play in ensuring the reputation and level of service provided are not damaged due to careless handling of personal or sensitive data.

What is a Data Breach?

'A breach of security leading to the accidental or unlawful destruction, alteration, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'

The biggest source of breach, in any organisation, is when communicating via email. It is easy to become complacent when using something so regularly but the sharing of files or data within emails is a form of 'data transfer' and should be secure at all times.

Things to consider when sending an email:

1. Always check you have the correct recipient address before hitting send.

2. Wherever possible, try to avoid using the 'auto-fill' function or if it is being used, double check the address before sending.

3. When sending bulk emails to an external list or to a list of students, ensure that the 'Blind CC' or 'BCC' address field is used. This will ensure that email addresses are not shared without authorisation.

4. Consider the email chain and the contents of pervious emails, which may contain personal or sensitive data. The default setting is to include the previous emails in a chain, however, this setting can be changed and previous emails not included.

5. Check attachments before sending. Some data breaches occur where the incorrect attachment is included or an unedited attachment etc.

6. When you are required to share and/or communicate personal/sensitive data, ask yourself the question 'Is there a more secure way for me to do this?' There are other sharing platforms such as Microsoft SharePoint, QUB's own Dropbox, the encryption of emails, the password protection of file attachments etc. which could reduce the risk further.

If a data breach has occurred, or you suspect has occurred, contact the Information Compliance Unit immediately at **databreach@qub.ac.uk**

Devices, Storage and Access

All portable QUB devices **MUST BE ENCRYPTED**. This can be done via Information Services.

Ensure that your devices have the appropriate login password controls and **NEVER** provide others with your logon credentials.

When storing or processing personal or sensitive data using a third party service consider the location of any servers for services offered. Transfers of personal data outside of the EEA (European Economic Area) are restricted and require adequate safeguards to be in place. Contact the Information Compliance Unit for advice **info.compliance@qub.ac.uk**

Always consider the access requirements and restrictions which are in place for document storage, with only those required to see it having access to it. Consider utilising the access controls already in place for SharePoint or Q Drives and ensure that any physical copies are kept in secure locked filing cabinets and not left on desks or publicly accessible areas.

If you require any assistance with the use of email, the handling of data, sharing or any other data privacy implications of your business processes, please contact the Information Compliance Unit **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**