Queen's University Belfast

# Providing and receiving personal data


www.qub.ac.uk

# Protect personal data during telephone conversations by:

- Asking the individual, where possible, to submit their request in writing via their organisation's email system or company headed paper.
- Identifying the person clearly.

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.

# Protect personal data sent in the post by:


- Checking to ensure that the address you are using is correct and up-to-date.
- Sending documents to a named person if at all possible – not to a department or team.
- Always putting a covering letter marked "Strictly Private and Confidential", with your contact details in the envelope with the information.
- Sealing the envelope securely and marking it "Private and Confidential".
- Sending documentation containing sensitive personal data by Royal Mail 'Special Delivery' or by courier.
- Writing your return address on the back of the envelope.
- Ensuring 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.

**IF IN DOUBT, DO NOT DISCLOSE ANY PERSONAL INFORMATION.**

# Protect Personal Data sent by email by:

- Always checking that you are using the correct and most up-to-date email address.
- Turning off the "Auto-Correct" feature in Outlook when you are processing personal data.
- Using the BCC (Blind Copy) function unless you are **certain** that recipients need to know who the other recipients are.
- Double-checking that you have added the correct attachment before sending an email.
- Ensuring any attachment containing personal data is password-protected.
- Contacting the recipients separately to provide the password if sending a password-protected document.
- Ensuring that the content is accurate and that language and tone of the email is professional and appropriate.

# Protect personal data held electronically by:

- Saving personal data in secure areas i.e. secure network drives.
- Locking your computer screen any time you leave your desk.
- Changing your password regularly and not sharing your passwords with colleagues.
- Using secure photocopiers/printers when working with personal data.
- Angling computer screens in a way so that people walking past cannot view the detail displayed on them.
- Ensuring that laptops, mobile devices and USB sticks, which may contain personal data, are encrypted.

# Police Requests

All Police requests for personal data must be notified to your line manager and immediately forwarded to the Information Compliance Unit. The Unit will take responsibility for issuing the University's response. Urgent out of hours requests made by the Police should be immediately forwarded to the Security Control Room for approval by the University Security Manager.

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

**Email:** info.compliance@qub.ac.uk

**Tel:** 2505 / 2506