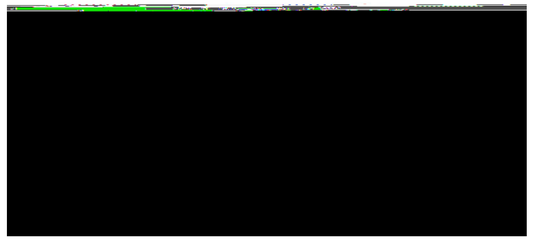
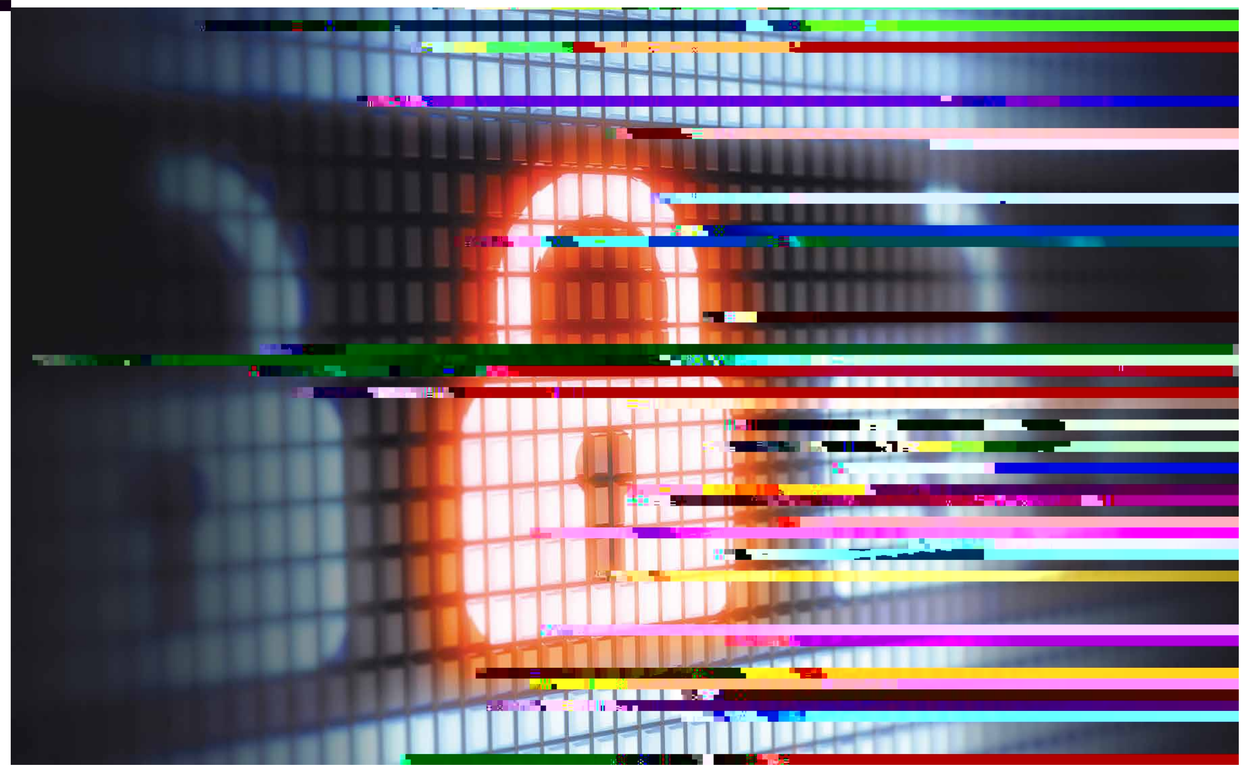


DIGITAL & INFORMATION SERVICES



What about email?

Sensitive data should not be sent by email. If you do need to use email, remember:

- Confidential files should be encrypted before being transferred by email
- Never use a personal email account for University business
- Take care that the recipients of the email are the correct recipients and have the authority to view the data
- Never submit login details in response to an email

What if I need to work away from the o□ce?

Under the Data Protection Act, the University is liable for the loss of data by theft. If you need to take or remotely access data off-campus, remember:

- Inform your line manager or supervisor before you take data or equipment off-campus and, if necessary, carry out a risk assessment
- Never leave documents, laptops or other devices unattended in public
- Do not use your personal computer, laptop or mobile device to store restricted data
- Sensitive data stored on a University laptop or mobile device must be encrypted
- Install theft recovery/protection software onto laptops and mobile devices
- Public wireless networks are less secure than the University's network environment
- When connecting remotely, ensure that your device is password protected and has an active firewall and up-to-date anti-virus software
- Report the loss of any device containing sensitive data IMMEDIATELY to Information Services by emailing itservicedesk@qub.ac.uk
- Protect smart phones/tablets with a PIN

What do I do if something goes wrong?

If something happens that could lead to personal or confidential information getting into unauthorised hands, or if you have ANY concerns about data security or suspect that a breach may have occurred:

- Inform your line manager or supervisor immediately, identifying the nature of the breach and the type of data involved
- Take any immediate steps you can to close the breach and minimise the potential impact
- Contact Information Services by emailing abuse@qub.ac.uk

For more information about data security, including the University's acceptable use and information security policies, visit: http://go.qub.ac.uk/itpolicies

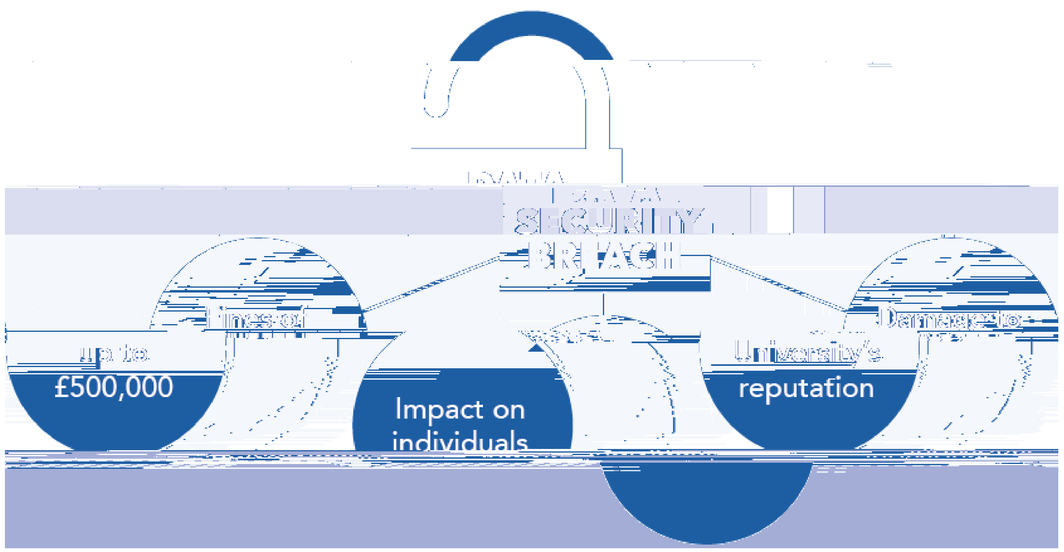
Advice on the transfer of data, encryption and the secure erasure of data is available from Information Services sta□ or from School-based Computing O□cers.

DATA SECURITY AT QUEEN'S

Essential Information for Staff and Research Students

What has data security got to do with me?

As an employee or a research student at Queen's, you may need to work with sensitive data, including information about research, students and staff. You have a responsibility to protect the confidentiality and integrity of the information that you access. If you don't think carefully about how you store and use data, you could find yourself involved in disciplinary action or legal proceedings.



What kind of data are we talking about?

Information which needs to be carefully handled may include:

- Data relating to individuals such as staff, students or research subjects
- Information given in confidence
- Financial information
- Details of research activity or intellectual property
- Information relating to exams or assessment
- Any other information not intended for the public domain

What can go wrong?

Research has shown that data breaches in Higher Education are often due to:

- Unauthorised access to data (both deliberate and accidental) by staff or other individuals
- Confidential or personal information being accidentally made available online
- The theft or loss of documents taken out of the office
- The theft or loss of a laptop, mobile device or storage device (such as a USB drive)

Sta and students should report data security incidents or threats IMMEDIATELY to their line manager or supervisor and email abuse@qub.ac.uk

The University's policies and regulations regarding acceptable use and information security can be found at: http://go.qub.ac.uk/itpolicies

What can I do to protect the data that I use at work?

There are several simple steps that you can take to protect your personal details and any data that you are working with. Remember:

- Create strong passwords that use a combination of letters, numbers and symbols
- Use unique passwords for each account
- Never reveal your passwords to anyone
- Password protect sensitive documents and store them on a secure network drive
- Use Ctrl+Alt+Del to lock your workstation before leaving your desk
- Keep confidential documents locked in a filing cabinet or drawer when not in use
- Lock your office door if there is nobody there
- Familiarise yourself with the University's Data Protection Policy