Best practice cybersecurity measures

- Keep your account password/access codes safe from others, including family and other household members.

- Ensure software and operating systems are regularly updated to protect your PC, laptop and other mobile devices from viruses and other cyber attacks.

- Make sure to lock your PC, laptop and other devices when unattended and be mindful of so called ‘shoulder surfing.’

- Be vigilant about ‘Phishing’. This is an attempt to obtain sensitive information such as usernames, passwords, and credit card details for malicious reasons, by disguising as a trustworthy entity either through email or over the phone.

- Ensure you familiarise yourself with the relevant IT policies, including but not limited to the IT Acceptable Use Policy
  [www.brookes.ac.uk/it/information-management/policies-procedures-legislation](http://www.brookes.ac.uk/it/information-management/policies-procedures-legislation)

- Securely dispose of paperwork and IT assets to ensure that information remains confidential.

- Securely transfer information to ensure it remains confidential where appropriate, by using University approved encryption software where required and be vigilant around the use of email forwards, USB sticks and other storage devices.

- Make sure your mobile phone is securely protected by either a pin number, password or fingerprint scan.

ISO 27001 - achieving cybersecurity maturity

The two year project to achieve this accreditation shows the University’s commitment to information security at all levels. Colleagues, students and parents can be confident that all University information captured and stored is validated by an internationally recognised framework.
Data Protection Act 1998 and Freedom of Information Act

Anyone can make a request for information (FOI) through the Freedom of Information Act 2000:
www.brookes.ac.uk/it/information-management/foi

Under the 8 principles of the Data Protection Act 1998 we have an obligation to protect information and individuals have the right to a copy of the information that is held about them by means of a Subject Access Request (SAR):
www.brookes.ac.uk/it/information-management/data-protection

Eight data protection principles

1. Personal information must be fairly and lawfully processed

2. Personal information must be processed for limited purposes

3. Personal information must be adequate, relevant and not excessive

4. Personal information must be accurate and up to date

5. Personal information must not be kept for longer than is necessary

6. Personal information must be processed in line with the data subjects’ rights

7. Personal information must be secure

8. Personal information must not be transferred to other countries without adequate protection

The Information Compliance Team

Is your primary point of contact to report an information security incident or make a Subject Access or Freedom of Information Request:
www.brookes.ac.uk/it/information-management/reporting-an-information-security-incident

We can be contacted by email on info.sec@brookes.ac.uk or by phone on #4354

References and Policies

IT Services Information Management team homepage:
www.brookes.ac.uk/it/information-management

Relevant policies:
www.brookes.ac.uk/it/information-management/policies-procedures-legislation

Information Commissioners Office:
https://ico.org.uk