Cyber Security and Data Protection Guidance

Best practice Cyber Security measures

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

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

3. **LOCK YOUR DEVICE.** Make sure you lock your PC, laptop and other devices when unattended and be mindful of ‘shoulder surfing’.

4. **PHISHING AWARENESS.** Be vigilant of ‘Phishing’ attempts; 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.

5. **POLICIES.** Ensure you familiarise yourself with the relevant IT policies, including but not limited to the [IT Acceptable Use Policy](https://search for Information Security on Brookes Webpage).

6. **DISPOSE CAREFULLY.** Securely dispose of paperwork and IT assets to ensure that information remains confidential.

7. **SHARE CAREFULLY.** 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.

8. **LOCK YOUR PHONE.** Make sure your mobile phone is securely protected by either a pin number, password or fingerprint scan.

Data Protection Act 2018 and Freedom of Information Act 2000

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

Under the principles of the Data Protection Act 2018 and General Data Protection Regulations we have an obligation to protect information and individuals have the right to get a copy of the information that is held about them by means of a Subject Access Request (SAR):

[https://www.brookes.ac.uk/it/information-security/data-protection---gdpr/](https://www.brookes.ac.uk/it/information-security/data-protection---gdpr/) Information about how to make a SAR can be found under “Data Subject Rights”.
PERSONAL DATA SHOULD BE:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and where necessary, kept up-to-date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
6. Processed in a manner that ensures appropriate security of the personal data.

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:
https://www.brookes.ac.uk/it/information-security/reporting-an-information-security-incident/

Can be contacted by email on info.sec@brookes.ac.uk or by phone on exn 4354

References and Policies

https://www.brookes.ac.uk/it/information-security/- IT Information Security homepage


https://ico.org.uk/global/contact-us/ Homepage of the Information Commissioner’s Office