St. Peter's College

Information Security Guidelines – Mobile Devices

Minimum requirements of Users:

- Make sure your device is password protected
- Ensure your device is physically secure at all times
- Use encrypted USB sticks and encrypt confidential and sensitive attachments to emails.

All members of staff who use mobile devices for work are responsible for ensuring that any personal, confidential, sensitive or restricted data is secure and that the integrity of the data is maintained. This is to prevent 1) data loss and 2) unauthorised access. Relevant information includes any personal data (see Annex 1), the loss of which might cause individuals damage or distress, and includes data about individual students, staff members and financial data. Users should also consider the security of the devices used to process data. These may include desktop computers, laptops, tablets, smartphones and portable storage media (e.g. USB storage devices (also known as datasticks), external hard drives and other removable media).

Data storage: Sensitive or confidential data should be stored and backed up on University-managed servers. Ideally data should not be copied to local devices without additional appropriate precautions. Data stored on University servers reduces the risk of unauthorised access and data loss (as data are typically backed up to multiple sites). Users should be aware of what back-ups are made for the servers they use.

Physical security: Users should be aware of physical security – e.g. unauthorised access to devices, including the risk of theft as well as dropping or misplacing devices and accidental damage. This needs to be the first consideration when ensuring that information is secure.

Remote access: Where sensitive or confidential data held in the University domain are accessed remotely, care must be taken to avoid local copies being held. The Oxford virtual private network (VPN - https://help.it.ox.ac.uk/network/vpn/index) can be used to enable data collected to be encrypted in transit and then stored & backed up on University servers.

Storage of data that is shared or outside the University: Sensitive or confidential data must be held in an encrypted form and users should be aware that many commonly used applications for storing or exchanging data may generate security risks unless appropriate steps are taken. Many useful web- or cloud-based services exist outside the University but use of these services often entails storage of data on servers that are outside the University's jurisdiction and potentially outside the European Economic Area. Examples include DropBox, iCloud, or Google Drive. If the data is sensitive, the user must ensure that any third party service allows them to meet their Data Protection responsibilities. Where data could be sent outside the EEA, participants should be informed of this fact (perhaps, during a consent process). If the service is in the US, ensure the provider has signed up to the "Safe Harbor Scheme". However, the nature of large-scale web- or cloud-based services often makes it hard for providers to be specific about data's geographical location during storage, processing and transit. For this reason, where equivalent IT Services services exist (OxFile- http://www.oucs.ox.ac.uk/services/oxfile/ - instead of DropBox), their use is encouraged.

Encryption: All devices that might be used to hold sensitive or confidential data must be encrypted. The University has implemented a PGP Whole Disc Encryption (WDE) service (http://www.it.ox.ac.uk/infosec/wde/). This service is accessed through local IT support staff. Portable/removable storage media such as USB drives holding sensitive or confidential data must employ hardware encryption. These work like normal USB devices, but require a password to access data and are available through your local IT support staff. The University WDE service is not currently appropriate for tablets and smartphones; advice on how to make these more secure is available – see Annex 2. Some devices may have built-in encryption capabilities.

E-mail: E-mail reflects an additional risk, and security should be considered on desktop and laptop computers as well as e-mail enabled portable devices such as tablets and smartphones. Any email enabled device should be password-protected with high password strength to prevent unauthorised access. If an e-mail-enabled device is lost, e-mail account passwords should be changed immediately. Security should also be considered when e-mail is forwarded to an external e-mail service. Any documents transmitted by e-mail containing sensitive or confidential data should be encrypted.

Password strength: A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or parts of the user's own name.

In case of any queries, contact SPC IT Support on 78881 or it-support@spc.ox.ac.uk.

Annex 1

What is personal data?

https://www1.admin.ox.ac.uk/dataprotection/oxonly/staffguide/

What is personal data?

Personal data is defined as:

'data which relate to a living individual who can be identified from that information, or from that and other information which is in the possession of or is likely to come into the possession of, the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (subject to very limited exceptions).'

In practical terms, an individual is 'identified' if he or she has been distinguished from other members of a group. This might be by means of name alone or name combined with other information (e.g. address, telephone number, date of birth etc). Sometimes, no name is necessary, for example if a particular combination of facts makes the person identifiable, or he/she is identifiable from photographs, video footage.

In a large and complex organisation such as the University, personal data is held on a large number of individuals (for example, current/prospective/former staff and students, and others with a connection to the University). It may be held in many places e.g. in paper files, on computers, in e-mails, in CCTV footage and photographs. It may also be held by a number of different people. All personal data held by the University is covered by the GDPR. It must therefore be held in accordance with the ten data protection principles and it is potentially disclosable in the event of a subject access request.

Annex 2

Advice for users on appropriate protection

InfoSec’s ‘Stay Safe on the Move’ site (https://www.infosec.ox.ac.uk/stay-safe-move
If you use a mobile device to store and/or transmit confidential University data and information (including via email), then your device(s) must be secured in accordance with the following principles:

1. Keep devices physically secure and take reasonable measures to reduce the risk of theft or loss (e.g. keeping the device on person and out of sight, don’t leave unattended in hotel rooms etc.)
2. Secure access to devices using an appropriate passcode, passphrase or similar; where appropriate default settings should be changed to allow use of more advanced passcodes
3. Set devices to automatically lock after a pre-defined period of inactivity (usually no more than a few minutes) and, where appropriate, to lock or wipe data if an incorrect password is entered too many times
4. Where appropriate, enable the ability to remote locate and wipe devices
5. Use TLS/SSL to access email (option when setting email account)
6. Keep software on mobile devices up to date with the latest version
7. Only install apps from trusted locations
8. Be careful who can read information when viewing in public areas
9. Report theft or loss of mobile devices to your department and the police
10. Remove University data when you leave the University