Exeter College Mobile Device Security Policy

1. Overview

Mobile working is recognised to bring benefits to any organisation. While laptops have been in mainstream use for a considerable time, the growth in the use of smart phones and tablets for both business and consumer use has enabled the College data to be used in more public locations, with the increased risk of personal information being viewed inappropriately and making it easier to lose devices and the sensitive data on them.

2. Purpose

The purpose of this policy is to provide adequate controls on the use and management of data on mobile devices.

This policy should be used in conjunction with the following policies

- Information Security Policy [INSERT LINK]
- INFORMATION SECURITY Incident Management Policy [INSERT LINK]
- Data Protection Policy [INSERT LINK]
- Acceptable Use Policy [INSERT LINK]
- Internal policies/procedures on data handing and data breaches

3. Scope

This policy is applicable across Exeter College and individually applies to:

- all individuals who have access to Exeter College information and technologies;
- "mobile device" applies to any mobile hardware that is used to access or store applications and data which originates in the College and for which the College is responsible , whether the device is owned by the user or by the College.

4. Policy

Information is critical to Exeter College's operations and failure to protect information increases the risk of financial and reputational losses. Exeter College is committed to protecting information, in all its forms, from:

- loss of **confidentiality**
- breach of its **integrity**
- loss of the **availability of data for the legitimate operations of the College**

Users and devices which fall within the scope of this policy should meet the following criteria.

4.1. Mobile Device Security

1. Users must ensure that any mobile device that is used to access Exeter College's data should have the remote wipe capability of the device turned on to protect against potential loss or theft.
2. Users must ensure that any mobile device must be protected from unauthorised access by, at the very least, a 4-digit PIN, a passphrase or a biometric lock and must be configured to ensure an automatic lock after a period of inactivity; two minutes is the recommended maximum length of time
3. Users must ensure that only trustworthy applications from reputable sources are installed.
4. It is prohibited to connect to the College network any mobile device that has undergone a 'jailbreak' procedure.
5. Users must ensure that all mobile devices are configured to receive software updates from the manufacturer. All updates for the operating system or other industry-recognised 3rd parties, which access or store college data should be installed within one month of release.
6. Users must regularly ensure that they clean their albums (for photograph, videos and multimedia files), deleted box, download folders, document folders, recycling bin and other similar virtual folders on their device to avoid memory space clog up. Devices with low memory may not be able to receive messages regarding software updates.
7. Users must ensure that mobile devices are not be used to carry sensitive data for any longer then absolutely necessary and must comply with the College's Data Retention Policy.
8. All College-owned Mobile devices ***must*** be encrypted to protect any data that is on the device. All personal devices ***must*** be encrypted if being used to store personal or sensitive data; this includes emails which may contain information about students or colleagues.
9. If the equipment is owned by the College, a record of all serial numbers and identifying information should be recorded.

If your device does not meet these criteria then no College data should be stored or accessed on the device. For the avoidance of doubt, this would preclude adding your College email account to the device.

4.2. Use of Personal Devices

Personal devices that meet the criteria above can be enabled to access the following services

- Eduroam/OWL
- Nexus Email
- The College Network via VPN and remote access
- University systems publicly available and protected by SSO
- Personal laptops may be connected to the College internal LAN providing they have up to date OS security patches, sufficient anti-virus/spyware/ransomware protection. They will only be permitted on a secure VLAN providing restricted access to College systems.

4.3. Use of College-owned Equipment

If you have been provided with a College-owned device then you are responsible for:

- Looking after the device with all due care and attention
- Ensuring the device is safe and securely kept

- Devices must meet all the security restrictions in 4.1
- All devices **must** be encrypted if they store personal or sensitive data.

4.3.1. Personal use of College-owned Equipment

Reasonable personal use is allowed, providing the use conforms to the College Acceptable Use Policy. Reasonable personal use includes, but is not limited to

- Internet Use
- Creation of personal data or documents.
- Entertainment

Exeter College takes no responsibility for personal data stored on College-owned devices. Data may be liable to be wiped remotely if the device is lost or stolen this includes, but is not limited to photographs, contacts and video recordings.

4.4. Lost or stolen devices

If any **personal or College-owned** device with College or University data on it is lost or stolen, this must be reported to Exeter College IT Department as a security incident. All efforts should be taken to notify Exeter IT at InfoSec@exeter.ox.ac.uk **immediately.** Where the loss or theft of a device may have resulted in a loss of personal data, no matter how small, this must **ALSO** be reported to the College Data Protection Officer (DPO) at dataprotection@exeter.ox.ac.uk **immediately**.

A remote wipe of the device should be triggered.

Users should ensure they change passwords for any system that was stored on the device, particularly their single log-on password for the University system, which included NEXUS.

4.5. Encryption

Enabling encryption and the options available will vary by device and operating system. The Exeter IT Department will assist with enabling encryption on your device. The basic settings should be:

- Encryption is enabled
- All disks/partitions/storage cards which store college data should be encrypted
- Where available default keys should not be used
- Where available Secure Startup/Boot should be enabled

5. Enforcement/Compliance

Wilful failure to comply with the policy will be treated extremely seriously by Exeter College and may result in disciplinary action.

6. Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Rector** is accountable for the effective implementation of this policy, and supporting information security rules and standards, within Exeter College
- **Governing Body** has executive responsibility for information security within Exeter College. Specifically, Governing Body has responsibility for overseeing the management of the security risks to Exeter College staff and students, its infrastructure and its information.
- **The Finance & Estates Bursar** is responsible for establishing and maintaining the Exeter College information security management framework to ensure the availability, integrity and confidentiality Exeter College information. The Finance & Estates Bursar will lead on

the definition and implementation of Exeter College's information security arrangements.

- **The IT Manager** is responsible for ensuring that security guidance is available for mobile device users and implementing technical controls to support the policy.
- **Users** are responsible for making informed decisions to protect the information that they process and implementing this policy on devices they manage.

Document Control

Policy Date	16th May 2018
Last Review Data	04th June 2019
Owner	Ian Williams

Version History

1.1	Approved	May 2018
1.2	DRAFT	04th June 2019