St Hilda's College
UNIVERSITY OF OXFORD

Mobile Device Policy

Contents

1. Introduction

1.1. This Policy is intended to ensure that St Hilda's College's security objectives are met in relation to the use of mobile devices, such as (but not limited to) smartphones, tablets, and computer laptops. Mobile devices represent a significant risk to information security and data security. If the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the College's data and IT infrastructure. This can subsequently lead to data leakage and system compromise. The College has a legal requirement to protect its information assets to safeguard users, intellectual property, and reputation.

1.2. This policy and associated guidance applies to:

1.2.1. Individuals who have been provided with a College-owned device.

1.2.2. Individuals (students, staff and visitors) who use a mobile device to access St Hilda's College information and technologies, whether or not the device is owned by the College.

2. Procedures for College-owned devices

2.1. In line with the University and College's rules and regulations regarding the security of other assets, the security of the mobile devices purchased by the College is the responsibility of the assigned user. The assigned user must read and have agreed to abide by this policy.

2.2. Standard mobile devices for staff will be acquired via the IT team.

2.3. Personal calls made by a mobile device provided by the College should only be used in emergency situations and call time kept to a minimum. In the light of download limits on devices and possible excess charges on tariffs, the line managers and the IT Manager will liaise to ensure that an appropriate SIM and tariff are procured. Any abuse or extensive use of the mobile device for personal use may be treated as misconduct. In cases where a mobile device is used as a team phone, the manager of the team must take overall responsibility. The assigned user will be responsible for payment of any mobile fines incurred (data or roaming charges).

2.4. Users must take responsibility for any additional software that they install, and any costs associated with such software, e.g. iTunes. The IT department cannot take responsibility for the effects of third-party software on the operation of any device unless the College's IT staff has been consulted beforehand.

2.5. If users need to add personal email accounts on their devices, they should use a different app for each account to segment work from personal, (e.g. Outlook for college business and other apps for personal use). They must take particular care to ensure that any College data is not sent through their personal email system.

2.6. Mobile devices in need of repair must be returned to the IT department who will check to see if a repair can be made; if this is not possible or cost-effective then the telephones will be returned to the suppliers for repair or replacement as appropriate. It must be noted that manufacturers' warranties do not normally cover damage caused by misuse, water, or neglect, and that the cost of such repairs could be borne by the assigned user.

2.7. Devices must not be "jailbroken", i.e., not have any software/firmware installed which is designed to gain access to any unintended functionality. (To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.)

2.8. Assigned users should ensure they follow protective security measures to reduce risk of data breach or cyber-attack. These include to:

2.8.1. Turn on remote-wipe capability of the device turned on to protect against potential loss or theft.

2.8.2. Protect from unauthorised access by using at least a 6-digit PIN or a passphrase.

2.8.3. Configure the device to ensure an automatic lock after a period of inactivity.

2.8.4. Only install trustworthy applications from reputable sources.

2.8.5. Configure the device to receive software updates from the manufacturer and other 3rd parties, and install updates within one week of being released. (In the case of tablet devices, these may need to be taken back to the IT department for the work to be carried out.)

2.8.6. Encrypt the device to protect any stored data.

2.8.7. Immediately report the loss or theft of the device to the IT Team, so that the risk of a data breach can be mitigated.

2.9. College IT reserves the right to perform a full remote wipe to all devices configured for access to College or the University systems (if the device is owned by the College) to ensure protection of the College's data.

2.10. When the assigned user leaves the employment of the College, the mobile device must be returned with its charger and any accessories to the IT department, unless agreement is given for the user to purchase the mobile device. If the assigned user has been authorised to purchase the device from the College, then all relevant College data, apps and control will be removed, prior to them taking the device. The IT department will not be held liable for any personal data (photos, documents, etc.) that may be on the device when it is given to the IT department. If the device is to be taken or given to an employee, then the College reserves the right to remove the current College mobile phone supplier account and to reset the device to factory defaults.

3. Guidance for non-College-owned devices

3.1. Staff, students and visitors who use their own devices to access the College's data or networks should ensure they follow protective security measures to reduce risk of data breach or cyber-attack. These include to:

3.1.1. Turn on remote-wipe capability of the device turned on to protect against potential loss or theft.

3.1.2. Protect from unauthorised access by using at least a 6-digit PIN or a passphrase.

3.1.3. Configure the device to ensure an automatic lock after a period of inactivity.

3.1.4. Only install trustworthy applications from reputable sources.

3.1.5. Configure the device to receive software updates from the manufacturer and other 3rd parties, and install updates within one week of being released.

3.1.6. Encrypt the device to protect any stored data.

3.2. A mobile device that has undergone a 'jailbreak' procedure must not be used to access the College's data; i.e., software/firmware which is designed to gain access to any unintended functionality should not be installed. (For the avoidance of doubt, to 'jailbreak' a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.)

3.3. The loss or theft of any mobile device that is used to access or store College data should be reported immediately to the Data Protection Officer and the IT team, so that the risk of a data breach can be mitigated.

4. Compliance

4.1. The College regards any breach of data privacy legislation, of this policy or of any other policies or regulations introduced by the College from time to time to comply with data privacy legislation as a serious matter which may result in disciplinary action.

5. Related policies

5.1. This Mobile Device Policy should be read in conjunction with related College policies and procedures, including with regard to Data Protection, Information Security, and Network Acceptable Use, and with University of Oxford Regulations Relating to the use of Information Technology Facilities (https://governance.admin.ox.ac.uk/legislation/it-regulations-1-of-2002).

**This policy was reviewed and approved by Governing Body
on 16 October 2024**