Wolfson College policy on the the use of mobile devices

WOLFSON COLLEGE
UNIVERSITY OF OXFORD

SCOPE AND REQUIREMENTS

The use of phones, tablets, laptops and other portable devices – whether personal or College owned - is permitted for all Wolfson College data, other than those listed exceptions, providing that devices are:

- Protected from unauthorised access by at least a 4-digit PIN or a passphrase;
- Configured to ensure they automatically lock after a period of inactivity;
- Configured in such a way that they can be remotely wiped in the event of loss;
- Encrypted;
- Only installed with trustworthy applications from reputable sources;
- Configured to receive software updates from the manufacturer and other 3rd partiesa nd updates are installed within one week of being released;
- Not a a jail-broken or rooted device;
- Not used to carry sensitive information for longer than absolutely necessary.

These requirements also apply when usernames and passwords that could be used to access College data are saved on the device (eg, for reading email).

RESPONSIBILITIES

Heads of Department are responsible for:

- The secure use of mobile devices in their department
- Communicating this policy to all users
- Identifying, documenting and communicating any exceptions

Users are responsible for:

- Keeping devices configured as per the requirements in this document
- Informing their line manger and Wolfson IT Support it.support@wolfson.ox.ac.uk if devices are lost or stolen

EXCEPTIONS

The following data are not authorised for use on mobile devices. If use of mobile devices is required specific authorisation must be sought from the Bursar:

- No current exceptions

The following exceptions to the requirements are permitted

- Where the device OS does not support Remote Wiping (notably Windows for PCs), this requirement can be omitted, if the use is registered with the IT Team.

This document is based on advice from the University's Information Security Team, who provide the tools, guidance and support for divisions, departments and colleges to implement effective local arrangements and adequately manage information security risk. They also monitor networks and systems to prevent and respond to external attacks. For more advice on securing your devices, systems and data see their website at www.infosec.ox.ac.uk

Wolfson College policy on the the use of mobile devices

WOLFSON COLLEGE
UNIVERSITY OF OXFORD

HOW TO

Here's what you need to do to meet the requirements on common mobile phones and tablets:

Set a PIN of at least 4 digits

- Settings > Passcode is set
- Settings > Security > Screen Lock is set to "PIN" or "Password"
- All Apps > Accounts > Sign-in options > Add

Configure auto-lock

- Settings > General > "Auto-Lock" is not set to "Never"
- Settings > Security > "Automatically Lock" is set to "5 minutes" or less
- All Apps > Settings > Personalisation > Lock Screen > "Screen times out after" is not set to "Never"

Set up remote wipe

- Settings > iCloud > Find My iPhone is turned on
- Phone is signed into Google account and location services are turned on
- Phone is signed in to Microsoft account

Encrypted

- Automatic when a PIN is set
- Automatic by default
- All Apps > Settings > System > Device encryption > On

Reputable Apps

- Only install apps from the Apple App Store, Google Play store, Microsoft Store, your handset's vendor or your mobile network provider.

Receiving security updates

- You do not need to do anything if you are using an approved device but you should monitor whether your vendor has ended support for your device and keep an eye on the list of approved devices.

Updates installed promptly

- Respond to prompts to apply updates within one week of availability and regularly apply updates to all apps.

This document is based on advice from the University's Information Security Team, who provide the tools, guidance and support for divisions, departments and colleges to implement effective local arrangements and adequately manage information security risk. They also monitor networks and systems to prevent and respond to external attacks. For more advice on securing your devices, systems and data see their website at www.infosec.ox.ac.uk