



USE OF MOBILE DEVICES

Scope and requirements

The use of phones and tablets – whether personal or College owned - is permitted for all 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 parties and updates are installed within one week of being released.

Responsibilities

Heads of Section are responsible for:

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

Users are responsible for:

- Keeping devices configured as per the requirements in this document
- Informing the College IT Manager and their line manager if devices are lost or stolen

How to


Here's what you need to do to meet the requirements on common devices:

Set a PIN of at least 4 digits

 Settings > Passcode is set

 Settings > Security > Screen Lock is set to "PIN" or "Password"

Configure auto-lock

 Settings > Display & Brightness > "Auto-Lock" is not set to "Never"



 Settings > Security > Secure Lock Settings > "Automatically Lock" is set to "5 minutes" or less

Set up remote wipe

 Settings > iCloud > Find My iPhone is turned on

 Phone is signed into Google account and location services are turned on

Encrypted

-  Automatic when a PIN is set
-  Automatic by default

Reputable Apps

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

Receiving security updates

- Check that your device is currently supported by the manufacturer, e.g. Apple or Samsung, and monitor this periodically. You can often find lists of supported devices on the manufacturer's website.

Updates installed promptly

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

Version control: V.1.0 (September 2018) DO