Mobile device policy
Version 3.0, December 2017

SCOPE AND REQUIREMENTS

The use of phones and tablets – whether personal or University owned - is permitted for all Blavatnik School of Government 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

The Head of ICT is responsible for:

- The secure use of mobile devices at the Blavatnik School of Government
- 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 ict@bsg.ox.ac.uk and their line manger 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 Head of Section:

There are currently no exceptions.

Blavatnik School of Government How to secure of mobile devices
Version 2.0, March 2017

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 (may be Touch ID and Passcode, or Face ID and Passcode)
- Settings > Security > Screen Lock is set to "PIN" or "Password"

Configure auto-lock

- Settings > Display & Brightness > "Auto-Lock" is not set to "Never"
- Settings > Display > "Sleep" is set to "5 minutes" or less

Set up remote wipe

- Settings > Apple ID > 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.

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