Mobile guidelines

1. Purpose and Scope

The University acknowledges that mobile computing and mobile devices (smartphones, tablets, laptops etc), whether university owned or personally owned, are a part of many people's daily lives and can be useful tools to support flexible working practices.

The University's Information Security Policy and the Guidelines for the Use of IT Facilities both cover use of systems and information via mobile devices. It is your responsibility to ensure that using your mobile device doesn't put you in breach of any University policy, especially when you are using or accessing restricted information. Protecting your mobile devices protects you and your information as well as university information. These guidelines have been created to help you comply with the Information Security Policy.

These guidelines are for all students and staff. They cover paper-based information when it is moved away from your usual place of work. They cover work you do both on and away from our campuses.

The following guidelines apply to anyone using mobile devices to access University systems or networks. They are general rules. You should also follow any additional rules, policy or guidance that is relevant to your particular Section, department or work area.

2. Guidelines

Securing your device

It is your responsibility to ensure that restricted University information you access on your device remains secure. You should:

- Ensure your device's operating system is up to date
- Ensure you have up to date anti-virus software on your device
- Make full use of any password or passcode facilities on your device.
- Set your device to lock automatically if it is inactive for a period of time
- Set your device to lock or delete all data if multiple attempts to log in fail due to an incorrect password.
- Encrypt information on your device wherever possible
- Disable Bluetooth and wifi capability when not using it and disable automatic connection to open, unsecured wifi networks.

Loss or theft of your device

You should ensure the security of your device at all times. If your device is lost or stolen you should:

- Use your device's remote locate and wipe facility
- Report it to the Helpdesk. If you are using OneDrive the Helpdesk may disable your device's access to the service.
- Change your network password and passwords for all University systems you have accessed from your device https://www.essex.ac.uk/password/login.aspx

Storing information on your device

You should avoid using your device for bulk or long term storage. You should:

- Delete emails and attachments as soon as you have finished with them
- Limit the amount of information that is synched to your device

Sharing your device

If you share your device with family members or friends you must ensure they cannot use it to access University information, including your University email. You should:

- Set separate profiles for different users of your device
- Log off from your profile when you stop using the device
- Not allow your device to remember passwords for any University systems and networks you access through it

You must never share your University passwords with family members or friends.

Disposing of your device

When you dispose of your device you should:

- Return the device to standard settings (“factory reset”)
- Delete any information from University systems and networks stored on it
- Unsynch your device from your University PC/computer
- Change your network password and passwords for all University systems you have accessed from your device https://www.essex.ac.uk/password/login.aspx

Leaving the University

When you leave Essex you must delete from your device all University-owned information from your device and unsynch your device from University computers, systems or networks. Your access to systems and networks will be removed when you leave.

3. Paper

Paper information can also be mobile, whether you’re carrying it to a meeting, between hot desks, or taking it home or to a conference to work on. As with the guidelines for electronic information, above, this is the minimum requirement for restricted information on paper. Your Section, department or work area may have additional rules that you should follow.

- Where possible use remote access rather than printing out large amounts of information.
- Secure lose sheets together to avoid losing any: put papers into an envelope, folder or bag to keep them together.
- If you are travelling with papers keep them with you at all times. If they have to be left in a vehicle, ensure they are out of sight.
- Lock papers away when you reach your destination.
- Shred papers after use unless they need to be returned to your workplace. Use a personal shredder or ask EMS Helpdesk to collect paper for confidential shredding.

4. Help and support

For help with physical security of your device, encryption, virus software, passwords and remote wipe contact the IT Helpdesk.

For advice and guidance on compliance with policy contact the Information Assurance Manager.

5. Non-compliance

Non-compliance with the Information Security Policy is a breach of the IT Guidelines for the Use of IT Facilities and can lead to disciplinary action.

Created: May 2016
Agreed by: ICT Steering Group 24 June 2016
For review: June 2019

Version	Comments	Date
1.0	First draft created by Information Assurance Manager	May 2016
1.1	Revised to incorporate comments from Assistant Director, ITS	June 2016
2.0	Approved by ICT Steering Group	23 June 2016
2.1	Updated to include some examples	13 July 2016