Edinburgh Napier University - Electronic Information Security Policy

Mobile Computing Policy

1.0 Scope

It is recognised by the University that mobile working is a necessary and often advantageous mode of working. However, mobile working today is now supported by a range of devices designed for ease of use and with the capability to connect and access resources such as email, online storage, and University business systems and data sources.

The purpose of this policy is to set out clearly what is required when using a University supplied or privately owned mobile computing device. Effective implementation of this policy will minimise the risk of data loss and/or inappropriate use or access to University electronic resources and information.

2.0 Policy

Before connecting your device to University Wi-Fi or other available networks you must ensure,

- You have installed a suitable anti-virus and malware protection software.
- You have registered your device with Information services for use on the University networks.

To ensure safe mobile working you should ensure,

- You have installed suitable encryption software for the storage and transportation of University information.
- University information should not be stored or transported using a mobile device unless there is a clear business need to do so and should be retained only temporarily to fulfil that need. After which the information should be adequately deleted and unrecoverable from that device.
- If the device is to be used to handle data provided by a third party, it is the device owner's responsibility to ensure any security or data handling requirements by that organisation are met.
- University information and critically any stored account, identity or access details must be removed before the device can be reassigned to another user.
- Users must ensure they mitigate the risks associated with the environment in which they may be working. Advice and guidance should be sought from information services on environments, off campus or international locations where you may be unsure of the risks you may be facing.

Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Users therefore must ensure the following,

- No University confidential information should be synchronised to or stored on cloud-based storage that has not been agreed contractually by Information Services on behalf of the University. This includes but is not limited to,
    - Drop box
    - Skydrive
    - SugarSync

Storage mediums and devices such as USB sticks, external hard drives, flash card and any other portable drives carry considerable risks in transporting, storing or transferring University confidential information and as such,

- Should not be used unless absolutely necessary to temporarily store University information.
- Encryption should be applied to all such devices.

Should the loss, theft or misplacing of any such device occur Information Services should be immediately informed via their help desk and should be accompanied with as much detail regarding the device, the data it held and whether the loss had been reported to any relevant authorities.