1. Introduction

1.1. This information security policy document sets out additional principles and expectations relating to using mobile computing devices and using computers away from the office. It is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- Confidential information - information which if improperly disclosed or lost could cause harm or distress to individuals, or financial loss or reputational damage to the University. This includes personal data, as defined by the Data Protection Act, and other valuable or sensitive information not in the public domain, such as information that is commercially confidential for the University or a third party, and information related to intellectual property.

- Mobile computing device – a portable computing or telecommunications device that can execute programs or store digital data. Examples: laptop, tablet computer (including iPad), personal digital assistant (PDA), smart phone, smart watch and other wearable computers, digital camera, CD, DVD, external/removable hard drive, USB memory stick or flash drive.

1.3. Mobile computing and telecommunications devices make it easy to work away from the office and thereby expose information to different and probably increased security risks. In particular, mobile devices are prone to loss or theft.

1.4. The availability of home computers and networked computers managed by third-party organisations can also enable staff or research students to process University information when away from the office. The University cannot assume, or ensure, that such devices have security controls adequate for secure handling of confidential information. Staff and students need to be aware of this and take responsibility for the secure processing of University information, wherever it is taking place.

1.5. Use of mobile computing to work securely with confidential data may involve additional cost and effort; this may be an unnecessary expense where suitable centrally administered services are already available. The business need should justify committing additional resources to mobile computing.

1.6. This document includes statements on:

- Mobile Computing.
- Information handling requirements.
- Mobile computing equipment - purchase, suitability and support.
- Management of mobile computing devices.
- Reassignment, repair and disposal of equipment.
- International transfer of personal data and the Data Protection Act.
2. **Policy scope**

2.1. This policy relates to storing and accessing University information:

- Using mobile computing devices.
- Using computers away from the office.

3. **Mobile Computing**

3.1. The University does not require staff or students to store or access confidential information using computing devices that it does not own or manage. Should the University require one of its members to use a mobile or home computing device to store or access confidential data, then a suitably configured University owned device must be provided.

3.2. Staff and students are strongly advised not to store or access any confidential information from: privately owned home computers, public computers in libraries, cyber cafes, hotels etc. This is because the University has no control over the specifications, operation or administration of such devices and therefore cannot be confident of their security.

3.3. Staff or students nevertheless electing to store or access confidential information from devices not owned by the University should take appropriate security precautions based on a risk assessment that takes into account the nature and quantity of the data involved. They should be aware that certain data supplied by external bodies may be subject to specific security requirements. In the event of loss or disclosure of confidential information, individuals responsible for handling that data will be expected to give an account of the security precautions in use.

3.4. Individuals must not allow any access to, or use of, equipment that may put confidential information at risk of loss or disclosure. Examples:

- Individuals must not permit others, including family or friends, to use or modify any equipment provided by the University to carry out their professional duties.

- Individuals, electing to take personal responsibility for storing or accessing confidential information using privately owned home computers, must ensure that others do not have access to or see that information. In addition they must ensure that unauthorised persons do not have privileges to install software or otherwise put the security of the system at risk.

3.5. Individuals who opt to use a mobile computing device not owned by the University to store or access confidential information are fully responsible for ensuring that the device features adequate security provisions in order to protect the information (see 6. Management of mobile computing devices).

3.6. Any loss, or possible unauthorised disclosure, of confidential information must be reported to the relevant Head of Department and Information Assurance Services.

4. **Information handling requirements**

4.1. Individuals must be authorised by the Head of Department to remove or send confidential information outside a secure University location, and a record must be kept of this by the department. Depending on the specific nature and quantity of the information it may also be necessary also to encrypt it. Refer to:

- **Cryptography Policy (ISP-S16)**
4.2. Unencrypted confidential information must not be transmitted via a network where traffic may be subject to snooping or interception. (Unless there is reason to believe otherwise assume this is the case.) Where it is uncertain that encrypted network protocols are in use from source to destination then encryption of data files before sending them is required. The data will then be secure regardless of whether all, none or only some of the stages in the network link use an encrypted protocol.

4.3. Where confidential information is being handled using a mobile device also:

- Where possible anonymise personal data.
- Handle the minimum amount of data necessary for the work in hand.
- Hold the data for the minimum time.
- Make backups. Mobile computing devices can fail, be damaged or stolen so have an appropriate backup regime for any important data stored on the device. Also ensure that backups are held securely, where possible on the University network.
- Use a password protected screen saver / screen lock. Should the device be left unattended this may help to avoid unauthorised access.
- Use strong passwords for all accounts which have access to the device. Weak passwords have been a major cause of compromised systems and data.
- Actively manage physical security and do not leave the device unattended where there is a significant risk of theft. Examples: do not leave it in a parked car, lock it in an office draw when not in use, lock the door when leaving it in an office etc.
- Do not leave the device logged in and unlocked where there is a significant possibility that it may be accessed by an unauthorised person.
- Do not work with confidential data where there is a risk of “shoulder surfing” i.e. someone looking over your shoulder at the screen or keyboard.

4.4. See also:

- Information Handling Policy (ISP-S7)

5. Mobile computing equipment – purchase, suitability and support

5.1. When considering use or purchase of a mobile computing device, that may be used to manage any confidential information, it is essential to ensure that:

- Where the device is to be used to handle data provided to the University by external bodies or vice versa, it is capable of meeting any specific security requirements demanded.
- The device is technically capable of providing acceptable security for data whether that data is being stored, downloaded or uploaded to the device.
- There will be adequate technical support available to ensure that the device can be configured and used in a way that keeps confidential data secure.

5.2. Advice and support for approved University devices and software may be requested from departmental computing staff or IT Services.

6. Management of mobile computing devices
6.1. To help ensure security, even on devices with full disk encryption, they must be actively managed in terms of configuration and maintenance. Encryption may not prevent access to data if a running full disk encrypted system is infected or hacked.

6.2. Ensure that devices have current and automatically updated anti-virus software installed. The presence of malware such as viruses or worms would be a threat to security of data on the device.

6.3. Ensure that the device remains up to date with security patches for both the operating system and any software applications installed.

6.4. Ensure that devices have correctly configured firewall software installed where applicable. Vulnerable network services would be a threat to security of data on the device.

6.5. Ensure user privileges are configured on the basis of “least privilege”. For example under Windows ensure that users that do not need administrator privileges are not in the “Administrator” or “Power Users” group.

6.6. Ensure that for normal business activities the user does not work with administrative rights. Administrative rights should be used only when it is necessary to perform specific system administration or configuration tasks.

6.7. Installing software from untrusted sources must be avoided. Such software is far more likely to harm security than tried and tested software obtained from well known legitimate sources.

7. Reassignment, repair and disposal of equipment

7.1. Departmental procedures must ensure that data is removed as appropriate before a loan mobile computing device is reassigned to another person. Preferably this should be done routinely at the time the device is returned.

7.2. Data must be securely deleted when disposing of mobile computing devices. Either a suitably effective in-house procedure may be used, or another organisation may undertake the work provided that they are subject to a contractual agreement stipulating secure data handling and deletion. (Note that simple file deletion is often inadequate for ensuring that files cannot be recovered. Staff needing to ensure that confidential data has been deleted are advised to seek assistance from their departmental Computer Officer or IT Services.)

7.3. Where a mobile computing device is to be repaired by another organisation there are two options relating to personal or confidential data stored on the device:

- Remove the data from the device before the repair or maintenance work is undertaken.
- Use a company that is subject to a suitable contractual agreement stipulating secure data handling.

8. International transfer of personal data and the Data Protection Act

8.1. Transportation of personal data to a country or territory outside the European Economic Area (i.e. the EU plus Norway, Lichtenstein and Iceland) potentially breaches Principle 8 of the Data Protection Act 1998. Staff and students need to be aware of this when travelling to countries outside of the EEA if they are holding any personal data belonging to the University on mobile computing devices. Accessing personal data that is stored on the University network via a mobile computing device, from a location outside of
the EEA, can also be problematic. For further information consult the University Data Protection Code of Practice and for advice contact Information Assurance Services.

8.2. Some countries (e.g. China and Russia) have specific restrictions governing the encryption of mobile computing devices that can run contrary to University policy, meaning that the solutions usually required may not be appropriate. For further advice contact IT Services.

**Failure to comply with University Policy may lead to disciplinary action.**

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.