Use of personally-owned IT devices and compliance with Information Security Policy

This guidance note provides advice on the security of University information held on personally-owned IT devices, including mobile devices such as laptops, iPads and other tablets, smartphones and storage devices including USBs and portable hard disk drives. The University's comprehensive Information Security Policy must be fully complied with at all times, in particular the Mobile Computing Policy and Cryptography Policy:
http://www2.le.ac.uk/offices/ias/resources/policies/ispolicy/strategic-policy/Mobile%20Computing%20Policy%20-ISP-S14.pdf
http://www2.le.ac.uk/offices/ias/resources/policies/ispolicy/strategic-policy/Cryptography%20Policy%20-ISP-S16.pdf

These policies outline that staff members assume full responsibility for the security of **personal, sensitive or confidential data** when it is processed on their personally-owned devices, and that stringent conditions will need to be met. This includes any information identifying students, staff or individual research subjects, and other non-personal information that is confidential or sensitive to the University in any way, for instance information not suitable for the public domain or access by third parties such as unpublished research data or writing, or information that is critical to the operation of the University.

There are a number of ways in which personally-owned IT devices can be used to store or access **personal, sensitive or confidential data** in compliance with University policy:

i) If using a non-encrypted personally-owned computing device you need to ensure that all files are only held on the University network (R, X or Z:drives) and remotely accessed, or on an encrypted storage device (see ii), and are not actually held locally on your own device unless the individual files are encrypted (see iv).

ii) It is acceptable to use a non-encrypted personally-owned computer to access files that are held on an encrypted storage device, e.g. USB stick or portable hard drive, as long as the files are only stored on the encrypted device and not locally on your own IT device.

iii) You could use your personally-owned computing device if it features functioning full-disc/hardware encryption, and other security conditions are met. Examples of the different conditions which could apply to different kinds of devices are:

- Strong password protection
- Current version of operating system
- Security patches applied
- App management controls
- Virus protection
- Auto-lock
- Auto-wipe
- Remote wipe facility
- Use of locate facilities
- Secure backup
- Secure disposal
- Security addressed in contracts (supplier, maintenance, cloud services)
- Controlled access by family/friends
- Security not undermined by jail-breaking of device
- Physical security measures
- Limit the amount of information held on the device
- Reporting any loss of the device to IAS.

iv) It would be acceptable to use a non-encrypted personally-owned IT device to work on files that have been individually encrypted. Word, Excel and PDF files can all be encrypted in their respective programmes.

Under no circumstances should personal, sensitive or confidential data be held on any personally-owned device where that information is not protected by encryption.

Please be mindful that when you delete a file from your own personal device it has probably not been conclusively deleted and could still be retrieved from the device. This illustrates why it is especially important that the information is protected by encryption if it is held on your device, even for a short period of time.

Further information can be obtained from Information Assurance Services: http://www2.le.ac.uk/offices/ias