1. Introduction

This document replaces “Guidelines for the storage of Sensitive and Confidential Data on Laptops and Memory Sticks Version 1 January 2009.”

These guidelines are aimed at staff storing sensitive or confidential University information on portable electronic devices, such as memory sticks and laptop PCs. It provides advice and information on how to secure this data so that if the device is lost or stolen, the risk of unauthorised viewing / dissemination is minimised.

A portable electronic device is always at risk of being lost or stolen when taken away from the office and there have been well publicised cases in the national media where this has occurred.

All staff are responsible for the security of any data and in the event that any such information is transported from the University will be expected to take all necessary steps to ensure its continued security. Guidelines for the storage of data are set out in this document and staff are expected to observe these as a basis for ensuring security of data for which they are responsible. In the event that security is breached, these guidelines would be evidential in terms of any decision to take further action including disciplinary action.

2. Confidential Data

Employees need to assess whether or not electronic data they wish to transport away from the office is confidential or sensitive. Typical examples are as follows, but this list is not intended as comprehensive:

- Researchers storing personal or company confidential information as part of a research project
- Administrative / Senior staff storing personal information (staff, students, others) or company confidential information (memoranda, financial data, etc) as part of their administrative work
- Confidential minutes from committee meetings
- Commercial in Confidence papers or reserved agenda papers

If after consideration it is considered necessary to take confidential or otherwise sensitive information away from the University on a portable electronic device, important requirements are that:
Any such information is a copy of an original stored on secure University filestore.
You have minimised the amount of information being removed.
Where possible you have anonymised this information so that it doesn’t identify individuals.
Confidential information taken in this way is protected from unauthorised access – as described in the sections below.

As a general point, all electronic information not transported off-site should be stored on University shared drives and not on the PC Hard Drive (C:). Should a PC hard drive malfunction or the PC get stolen, this information will be recoverable if it is stored on a University shared drive, since these shared drives are automatically archived by IT Services. If it is stored on the PC Hard Drive it may not be possible to recover the data.

3. Theft of Portable Devices

All thefts or loss of computers / portable devices / memory sticks must be reported to your Line Manager immediately. If data loss includes sensitive data, the Data Protection Officer should also be informed immediately.

4. CD / Floppy Disk

Confidential information should never be stored on CD or Floppy Disk, the University had no facilities to offer encryption or other security features to CDs or Floppy Disks. However, these devices are still usable for the storage and transportation of non-sensitive or non-confidential information.

5. Memory Sticks / USB Pen Drives

Memory sticks typically have no security; however, at additional cost, secure devices with password protection can be purchased. These devices offer high levels of security using built-in hardware encryption and password protection systems. In the event of the device being lost or stolen, it is unlikely that data on the device will be accessible. Files on these devices are encrypted but are accessible by typing in a password when the device is connected to a PC (running Windows 7/XP/Vista, etc). Staff wishing to transport confidential data on a memory stick must do so using one of these secure devices. Further details and ordering information are available from IT Services via the Service Desk.

6. Laptops

It is also possible to encrypt the data on laptops to provide similar high levels of security. IT Services can encrypt laptops using the TrueCrypt software which provides vastly improved levels of security with minimal disruption to the user. The encryption process is a one-off installation that will provide continuous security of any existing data stored on the laptop, as well as any new files created in the future. The encryption/decryption process is totally transparent and requires no user intervention apart from a single password entry at start-up. Staff with laptops containing confidential data that are used outside the University, should
use this service to ensure data is secured in the event of loss or theft of the equipment. The installation process will take several hours so it will be necessary to leave your laptop with IT staff while it is completed. Further details on this service and how to book an appointment are available from IT Services via the Service Desk.

Users running their Laptop using non Microsoft operating systems (eg Linux, MacOS) should contact the IT Service Desk for specialist advice about Laptop security and encryption.

7. Smart Phones and Tablets

At the time of writing, there are a wide range of portable devices available with varying levels of security. The advice here is correct at the time of writing but with a rapidly evolving marketplace for these devices, users are advised to contact the IT Service Desk for up to date advice.

Users of such devices are advised to avoid storing sensitive data on them and to be particularly cautious when considering the installation of third party applications.

As a minimum, such devices should be protected by a PIN or other built-in security feature.

8. Encryption Passwords

All encryption systems offered rely on the user entering a password to access the encrypted information. In the event that this password is lost or forgotten, the encrypted data will be unrecoverable. This is by design. It is therefore VERY IMPORTANT to use a memorable password or make a note of the password in a safe place – AWAY FROM THE DEVICE. In the case of the encrypted USB pens, you are allowed up to 10 consecutive attempts at entering the password correctly. After that the data is automatically destroyed.

9. Shutting Down Your Laptop/PC

There is a slight risk, even with encrypted laptops/PCs, that passwords and information can be accessed using so called “cold boot” attacks. To prevent this from happening, it is important to ensure that you shutdown your laptop/PC properly (using the Windows Shutdown procedure) and that it is completely powered off whenever you are not using it. Using “Hibernate” or “Standby” modes will mean your data is not fully secured and could still be accessed by others.

10. Working from Home

When working from home, it is important not to copy sensitive files from protected laptops and memory sticks onto your home PC, unless it too has the same level of protection. There are various snooping devices and methods available which would enable access to unprotected devices. Therefore sensitive electronic documents should only be held on the protected device.
If you work on files held on a memory stick, images of these documents will be stored in temporary areas on your PC. It would be prudent to use PC software to remove these temporary files when you have completed your work – especially for particularly sensitive files. This can be achieved using the Windows Disk Cleanup utility, as follows:

Click on “Start” (bottom left of your PC), click “Run” then type in: cleanmgr and press return.

A PC wizard will display a menu of item types which it could remove for you. Ensure all temporary file items types are ticked, click OK and click “yes” to remove the items. If you are unsure what to do, please contact the IT Service Desk for further advice.

In time it is hoped that individuals will be able to access their network drives from home, which would remove the need to transport data off site.

11. Identified Individuals working with Sensitive Data

The University has identified a number of individuals who are expected, as part of their daily working activities, to work with a high level of personal and confidential data.

Those individuals will receive tailored training on the use of encryption and suggestions for the safest ways to work with their data. For further details on this, please contact the Data Protection Office in Governance, Planning and Academic Administration.

12. FIPS 140 Encryption Standards

The Federal Information Processing Standard 140 (FIPS) are series of publications relating to computer security standards for encryption. They are most famously used by US government agencies to ensure as much as possible that the encryption methods they use are as secure as possible. However, other organisations often insist on encryption methods that meet the FIPS 140 standard as part of their data or communication requirements. At the time of writing, the current version of the standard is FIPS 140-2, issued on 25 May 2001.

If an organisation you are dealing with insists on data being encrypted using a FIPS 140 compliant method, then please contact IT Service Desk for advice as the solutions offered differ slightly to those above.