Using encryption to protect your data

What is encryption?

Encryption is a way of encoding information so that it cannot be read without the appropriate key to decode it. It is a way of rendering files, volumes or hard disks extremely secure.

When should encryption be used?

Encryption should be used to secure data that you need to keep private and that you wouldn't want exposed if the device the data is sitting on was stolen or lost.

What should be encrypted?

Aside from your own personal information, encryption should also be used when you are dealing with data (including the Data Protection Act's definition of *Sensitive Personal Data*) which the LSE would classify as 'Confidential'.

Evaluating what data are Confidential

You can read about LSE's Information Classification scheme here.

Confidential information includes someone's racial/ethnic origin, political opinions, religious beliefs, trade union membership, physical / mental health, details of their sexual life or their criminal record.

It is up to you to assess the data that you're using and take responsibility for the measures you use to protect them.

Using encryption on different devices

PC / Mac:

It's a good idea to make sure that your PC or Mac requires a username / password to log on anyway. Ensure the hard drive and any attached external hard drives or other removable devices that will store 'Confidential' data are encrypted.

External Hard Drives / Removable Devices

If you are going to put 'Confidential' data on removable devices, either the data **or** the device should be encrypted.

You can purchase hardware-encrypted external hard drives and flash drives should you need to store large amounts of 'Confidential' data.

You can also create encrypted volumes on external hard drives or removable devices, or create encrypted zip archives or individually encrypted files on removable devices.

Tablet / Phone

If you are using a tablet or a phone to store any Confidential data, we recommend that you make sure that the phone's storage is encrypted (which has to be performed manually on an Android phone or tablet. A simple 4-digit PIN only provides very weak encryption that is easily cracked.

Individual Files / Attachments

If you are emailing attachments containing 'Confidential' data we recommend that the attachments are encrypted. It is not a wise idea to include 'Confidential' data in the body of an email or in unencrypted attachments. The best practice is to distribute the passphrase to the encrypted attachment in a separate email.

Encryption Standards – what to use

The accepted standard is **AES 256-bit**. Not all encryption programs support this, so unless contractually stipulated, AES 128-bit, 3DES, or Blowfish, when combined with a complex passphrase, provide an adequate level of protection.

Encrypting volumes and disks - software

PC

Enterprise editions of Windows come with BitLocker as standard, which you can use to encrypt drives, disks and usb sticks.

Linux

Most versions of Linux come with built-in options for configuring Full Disk Encryption (FDE)

Macs

Mac OS X 10.7 (Lion) and more recent releases have FileVault functionality built in that can be enabled to encrypt the hard disk. See http://support.apple.com/kb/HT4790 for more information.

iPhones and iPads

Volume encryption is enabled by default on iPhones and iPads if PIN or passphrase access is configured.

Android Devices

Storage volume encryption is available as an option you can enable on Android devices. See http://support.google.com/android/bin/answer.py?hl=en&answer=1663755 for more details.

Encrypting individual files for use on a PC

Axcrypt

Axcrypt (http://www.axantum.com/axcrypt/Downloads.html) is intuitive and user friendly, but is limited to 128-bit AES encryption, and the files it creates cannot be opened on a Mac.

7zip

7zip (http://www.7-zip.org/) is less user-friendly but can create zipped archives with 256-bit AES encryption, that can also be opened using the unzip function on Macs. You can find instructions of how to zip and encrypt using 7zip here: http://www.medicalnerds.com/how-to-encrypt-zip-files-securely-using-7zip/.

Encrypting individual files for use on a PC or Mac

7zip

As mentioned above 7zip can create encrypted zipped archives that can be opened on PCs or Macs. Encrypted zip files created on a Mac should be able to be opened on a PC using 7zip. Instructions on zipping on a Mac are available here: http://operating-systems.wonderhowto.com/how-to/create-encrypted-zip-archive-mac-os-x-and-windows-0139565/. There are also 7-zip variants available for Macs which you can find here: http://www.7-zip.org/download.html

MEO Encryption

MEO Encryption Software (http://www.nchsoftware.com/encrypt/index.html) has a common interface for both Mac and PC users, and therefore is more user friendly than either 7zip or the Mac zip file encryption, but uses an older encryption algorithm: 3DES.

Encryption keys

The key to all encryption is the passphrase that is used to decrypt a file of volume. This is known as the encryption key. Losing or forgetting your encryption key will render your encrypted files or device unusable.

Countries which may request you hand over the key to any encrypted volume

The border agencies and police forces of some countries may object to the presence of encrypted files or volumes that they cannot decrypt. Government agencies in *any* country may demand you hand over the encryption keys or otherwise demonstrate what is contained within an encrypted folder. This may happen with or without any legal enforcement in place to encourage such a situation.

If you are travelling abroad with encrypted Confidential data this creates the risk that such data may be exposed to unintended recipients, breaching the Data Protection Act.

If the encryption software you are using is not a mass market product freely available to the public, you may need to obtain a Cryptography Open General Export Licence (OGEL) before travelling abroad with it. This will not be the case if you are using any of the products included in these *Encryption Guidelines*. See the UK Government's note on the export of Cryptographic items at https://www.gov.uk/export-of-cryptographic-items and for more information about OGEL rules https://www.gov.uk/dual-use-open-general-export-licences-explained.

The Wassenaar Arrangement

In theory, any citizen of a member country of the "Wassenaar Arrangement" may travel to any of the other countries who have signed the agreement with an encrypted device, under a "personal use exemption," which holds as long as that person does not create, enhance, share, sell or otherwise distribute the encryption technology whilst visiting.

Russia and Ukraine, whilst being signatories of the Wassenaar Arrangement, do not permit "personal use exemptions."

A list of Wassenaar Arrangement countries can be found here:
http://www.wassenaar.org/participants/index.html

Please note that a "personal use exemption" does not guarantee that a citizen of these countries will not be requested to hand over encryption keys.