Encryption

Encryption* adds another layer of protection around your data, and should be used if the data is sensitive.

There are a number of *encryption standards* available applying different algorithms while encrypting data/devices; confidential info should be protected with the 256-bit AES or above – see pg 2 for advice.

***What is encryption?**	*Encryption renders your data into an unreadable format, therefore without the knowledge of the encryption key an unauthorised access attempt could not get hold of any usable information. The intent is to maintain your data confidentiality and integrity (as the main elements of InfoSec) when it's at rest or in transit.*
***When do you need it?**	*It depends on the nature of data whether encryption is needed; confidential data and sensitive personal information in the context of UK Data Protection Act should be encrypted if held outside LSE network.*
***How can it be applied?**	*Encryption could be applied to both the data files, and devices accessing such data.* *You need to set your encryption key while encrypting the data files/devices. An encryption key is the password used to decrypt the encrypted data or devices.* *Any encryption is only as strong as the password chosen.*

IRON RULES PROTECT ALL OF YOUR DEVICES AND DATA

File encryption

7zip **(http://www.7-zip.org/) as a compression tool can create zipped archives with 256-bit AES encryption, which can be opend on PCs or Macs**

Axcrypt **(http://www.axantum.com/a.xcrypt/Downloads.html) can provide 128-bit AES encryption, which can be opened on PCs but not Macs**

Window's *Encrypting File System (EFS)* (http://windows.microsoft.com/en-gb/windows/what-is-encrypting-file-system#1TC=windows-7) provides AES and 3DES encryption (not secure prior to Windows 7)

Mac users can also download *iZip* (http://www.izip.com/) which can provide 256-bit AES encryption to zipped archives.

OS X's built-in *Disk Utility* (disk repair and management tool) can also encrypt volumes and drives (OS X can create a compressed volume just by right-clicking the file or folder)

[NOTE] *TrueCrypt as a popular encryption tool was announced as no longer secure by its developers in 2012 and support was ceased.*

Full disk encryption

Windows PC

BitLocker comes with Windows Vista, 7 and 8, which could be used to encrypt the drives, disks and USB sticks

Macs

FileVault as a built-in functionality could be enabled to encrypt the hard disk *https://support.apple.com/en-gb/HT204837*

Linux

Most versions of Linux come with built - in options for configuring Full Disk Encryption – see below links for advices:

Arch Linux devices; Fedora Linus devices

RedHat Linux devices; Ubuntu Linux devices

iOS devices

iOS devices provide the 'Data Protection' feature which offers hardware encryption and facilitates a fast secure erase of the device in case the device is lost/stolen: https://support.apple.com/en-gb/HT202064

Android devices

Android devices provide storage encryption which is same as your phone's lock-screen PIN/password. Storage encryption is one-way only that you can only disable encryption by resetting your phone to its factory default settings

https://support.google.com/nexus/answer/2844831?hl=en-GB

External hard drive, removable media

BitLocker *can be used to encrypt external hard drive and USB sticks*

Alternatively you can purchase external hard drive/USB stick with hardware based encryption e.g. iStorage datAshur