BUSINESS CRITICAL DATA

Guidance on Electronic data: http://www2.lse.ac.uk/intranet/LSEServices/IMT/infosec/home.aspx
Guidance on Physical data:
http://www2.lse.ac.uk/intranet/LSEServices/legalandCompliance/recordsManagement/Home.aspx -

Data in the School:
The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning and good governance of LSE. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for LSE to recover.

Confidential Data:
Any security breach of confidential data will be handled in accordance with all relevant School policies. Any security breach which also involves data classified as Confidential under the Data Protection Act may result in legal action being taken against the School and disciplinary action against an individual or individuals.

Classification of Data:
Not all critical data is confidential data. You can find the School's data classification policy here: http://www2.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/infoSecClassification.pdf

If you are unsure or require further information please see the websites above or contact the School's Information Security Manager/Records Manager.

Electronic Use of Confidential Data:

PC/Mac/Laptop:	Ensure an explicit username password is needed to log on. Consider using a power on password to deter theft of remote data.
External hard drives / removable devices / USB sticks:	These devices should be encrypted.
Tablet/Phone/Ipad:	Storage should be encrypted and a passphrase should also be required to access the information.
Emails / email attachments:	Emails can be easily intercepted and read. Any attachments should be encrypted.
Cloud/Dropbox etc:	Internet document transfer tools can be vulnerable. The School provides explicit guidance to the use of these internet based programmes at http://www2.lse.ac.uk/intranet/LSEServices/IMT/guides/softwareGuides/other/using-dropbox-cloud-based-services.aspx
Travelling with encrypted confidential data:	Some countries may demand that you hand over your encryption keys. Check before you travel and contact the Information Security Manager for further information.

Storage of Confidential Data:
Electronic data: the storage of data classified as confidential differs from that of critical data. Check the data classification policy, and if you need further help or advice on storage contact the IMT IT Service Desk.

Physical data: Hard copy records that require protection for business continuity purposes will have the following characteristics:

- They are originals
- They have legal status
- They relate to outstanding payments to the School
- They are handwritten, or mainly handwritten
- They are in ledgers

To safely store it consider the following methods:

- Make sure you store your data in a secure location that is fire and water proof.
- Consider investing in a fire proof document safe to hold confidential files, such as exam scripts, student loan agreements, contracts etc.
- Store documents in the School's offsite record repository if they are not in regular use. The Records Manager will be able to advise on this.

Back Up of Business Critical Data:

Electronic Data:

- Do not store data one place but have multiple copies, on external hard disks or writable DVDs.
- Make sure that you store all copies of your data in a secure location and that material is encrypted and devices passworded.
- Keep paper copies of essential IT records.

Physical data: (for more information see the website above or contact the Records Manager)

- Scan critical documents and store electronically.
- Keep back up copies in a secure fire and water proof location, e.g. a safe.
- Have off site back up copies e.g. in the School's external records depository, or in a securely locked facility in a key team member's home.

How Long Should Data be Retained?:

The School policy on how long data should be retained is outlined here: http://www2.lse.ac.uk/intranet/LSEServices/legalAndCompliance/recordsManagement/retentionSchedules.aspx

Safely Disposing of Business Critical Data:

At the time of writing the School's policy on disposal of data has not been finalized. However, you should be aware that just deleting electronic data does not necessarily wipe it off your systems and you may need to overwrite it several times (the US Department of Defence recommendation is 7 times). A free tool such as 'eraser' (http://eraser.heidi.ie/) can do this.

In terms of physical data, Environmental Services oversee the confidential waste service contract, but it is the porters that can deal with any requests for confidential sacks and organise for their collection and destruction. The main issues are to ensure that confidential waste sacks are picked up as soon as possible and kept in locked places before being picked up e.g. not in publicly accessible corridors. CDs and DVDs can be cut up but take care that you wrap up any sharp edges or let the cleaners know that they should take care when disposing of rubbish bags containing any shards.

Good Housekeeping:

All members of staff who create, store, receive and use records must:

- Treat records as a School resource;
- Ensure as far as practicably possible that records are accurate and filed in such a way that they can be easily located;
- Keep records no longer than they are needed;
- Keep confidential records in a secure environment;
- Keep records stored in a safe and cost-effective way;
- Allow people to access information only if they need or have a right to do so;
- Create records that are accurate and that do not defame another individual, expose the LSE to unnecessary risk or to tamper with records in a way that risks them becoming inaccurate;
- Save long term records in an open source or archival format to ensure readability even if systems change