Research Data Guidelines

There are a number of areas that need to be considered when storing electronic data which are summarised below.

- Ownership & Lifecycle Management
- Confidentiality
- Criticality
- Availability

Ownership & Lifecycle Management

The ‘owner’ of each section of data needs to be identified. The owner is responsible for authorising access to the data, maintenance, accuracy and destruction when no longer required. A data owner is normally defined by role (e.g. PI on a research grant or PhD student).
Further information can be found here: http://goo.gl/t2SRA.

Confidentiality

Data needs to be adequately protected such that both the risk of reputational damage to the University and the impact on any individual whose personal details are recorded are minimised if it were to be disclosed to a person or persons not authorised to view it. Both the likelihood of disclosure and the impact of that disclosure need to be considered. For example:

Description of Data	**Storage Location**	**Likelihood**	**Impact**	**Mitigation Factors**
Anonymised transcripts of interviews about working in Higher Education	N: drive only	Low	Low	None required
Transcripts of person identifiable interviews about working in Higher Education	M: drive only	Low	Med	None required
Database of sex offenders containing person identifiable data	N: drive only	Low	V. High	Encryption required on N: drive folder (exceptional circumstances)
Results of survey about working in Higher Education containing person identifiable data	Laptop then N: drive	High	Med	Encryption required on laptop, but not N: drive folder
Anonymised responses to online survey	Laptop / USB memory stick	High	Low	None required
Data which has a significant commercial value to the University	Laptop then N: drive	High	High	Encryption required on laptop but not N: drive folder

General guidelines are as follows:

Encryption, portable devices and Data Protection Act

1. Only highly sensitive data stored on the M: or N: drives needs to be encrypted. Please check with your Faculty IT Manager if you believe that your data falls into this category.
2. Any data stored on portable devices (laptops, memory sticks etc.) that would cause the University to suffer any kind of reputational damage (or an individual to suffer personal loss) if disclosed to unauthorised persons (through loss / theft of the device for example) should be encrypted. This includes data covered by the Data Protection Act 1998 (as defined in sections 6-8 of the University policy on data protection) See http://goo.gl/2kemW for examples of such data.
3. If you store data on a portable device, it should be encrypted using the University Encryption Service software (http://goo.gl/0lWSw) unless that device is **only** used to store data which would result in a low impact on the University's reputation if disclosed. Examples of such data would include survey results that do not identify individuals or anonymised interview transcripts (both of which also have little or no commercial value to the University)Keep personal passwords secret; never disclose or share them. Group passwords must not be disclosed outside the group.
4. Never leave a computer logged on and unattended unless it is locked with 'password protection'.
5. Comply with The University's Code of Practice on Data Protection (see http://goo.gl/2kemW) In particular do not keep data longer than needed for the conduct of University business.

e-mail

6. Never redirect or forward emails in your University Outlook account to an external e-mail account (for example, a personal hotmail account).
7. When e-mailing other members of the University, always use their University e-mail address rather than externally-hosted e-mail facilities.
8. When sending emails, always double-check that you have used the right address before sending.
9. When you are off campus, use only Outlook Web Access or Citrix or another University-approved system to access University e-mails or data.

Physical Documents

10. Transport paper documents containing confidential or highly confidential data only where absolutely necessary, keeping them to a minimum and secured about the person in a locked case. Ensure appropriate security controls are in place if documents cannot be returned to the University over night.
11. Use shredding machines for disposal of confidential and highly confidential paper documents. Dispose of unwanted computer hardware only through Cleaning Services. Seek advice if you are unsure what to do.
12. Ensure offices are locked when they are unattended, and that confidential and highly confidential papers are locked away when not in use.

Working with Third Parties

13. Make sure any third parties permitted to handle data are required to take appropriate security measures. You must also check with your Faculty IT Manager if you intend to collect any data outside the European Economic Area (http://goo.gl/TTLWA).
14. Respect any additional third party rules relating to data that has been shared with the University – for example, by the NHS.

Other

15. Attend appropriate training.
16. Further advice on what types of data need to be encrypted can be found here: http://goo.gl/5VBh6
17. The University standard on data encryption is available here: http://goo.gl/wUM9A

Criticality

The criticality of the data is determined by the impact of it being lost or corrupted. If the permanent loss of the data would be anything other than a minor inconvenience, then it should be backed up effectively and reliably. Data stored on the M: or N: drives is protected in this way. Some faculties also run local storage and backup service and will advise you how to access these if appropriate.

General guidelines are as follows:

1. It is generally **not** sufficient for data to be stored on the hard disc (e.g. C: drive) of a desktop computer, even if a copy is taken periodically onto a portable hard drive / flash disk or similar (unless total and permanent loss of that data would be no more than a minor inconvenience or your Faculty IT staff have confirmed that data stored in this location is backed up automatically by local IT systems).
2. If you store data on the M: or N: drives, then it is fully protected and there is no requirement to (and you are advised against) taking a local backup as well.
3. Data on the M: or N: drives can be accessed remotely via http://access.leeds.ac.uk
4. Further information can be found here: http://goo.gl/5VBh6

Availability

Even if your electronic information is adequately protected by a full backup service, then the impact of it being unavailable for a period of time (due to service failure or the need to restore from a backup) needs to be considered. This is especially important if you are working with partners in other countries (who may need to access the data outside normal UK office hours when maintenance and service disruption usually occurs). The impact of longer term unavailability of the data also needs to be considered, as it could take several days or even weeks to fully restore a file system from backup tapes if a major incident (such as a fire) were to destroy one of the campus data centres.

Other advice

Research data that needs to be accessed by more than one individual should normally be stored on the N: drive, unless your Faculty IT staff advise you otherwise. This makes it easier to give access to the data to others if required and also minimises the impact to the project if staff leave the University. It is important to notify your Faculty IT Manager as early as possible if you need to store large amounts of data (i.e. over 10Gb).

All security incidents or breaches must be reported immediately to the University IT Security Coordinator, Kevin Darley (k.j.darley@leeds.ac.uk / 0113 343 1118).

Your Faculty IT Manager, can provide further help and advice on any aspect of data storage.