Data Protection and Research

Adrian Slater & Professor Louise Dye

“The things people want to know about are usually none of their business”
(George Bernard Shaw)

These slides and related presentation do not constitute legal advice. Specific legal advice should be taken for acting on any topics covered.

DP and Research 2018 - GDPR
Human Tissue Act
(where you use human tissue)

- Valid consent (don’t forget the personal data!)
- Don’t always need consent if tissue from living person, does not identify patient and REC approval

Guidance: HTA code of practice on research code E
https://www.hta.gov.uk
Freedom of Information Act
(Who can get to see your research?)

- Freedom of Information requests
- Exemptions:
  - Section 40 if data “personal data”
  - Section 22 “for future publication”
  - Section 22A information from a programme of research still underway

Breach of confidence

- Breach of confidence three elements? (*Coco v AN Clark Engineers 1968*)
- Article 8 Human Rights Act
  - Right to respect for private and family life
- When is it ok to breach confidence?
  - Public interest and vital interest of the subject

In interview a data subject tells you something that could be very damaging to themselves or another, what can you do?
Breach of confidence (cont’d)

● “Best endeavours to keep confidential” – what does that mean???
● Does confidentiality cover the deceased?
● Can you still share with another researcher?
Research Ethics Committees

- Standard application forms and template consent forms
- New forms addressing new privacy notice requirements and privacy impact assessments

Guidance:
http://ris.leeds.ac.uk/downloads/2/good_practice_and_ethics
Data Protection Laws

- Data Protection Act 1998
  - New Data Protection Bill
- General Data Protection Regulation (GDPR)
- What about Brexit?
Legal Risks

- Information Commissioner’s Office (ICO)
  - Supervisory authority
- Rights of compensation for data subjects
- €20,000,000 or 4% of global turnover!
- Personal criminal liability if “intentionally or recklessly re-identify individuals from anonymised or pseudonymised data” and “altering records with intention to prevent disclosure following a subject access request”
Legal Risks

- Hertfordshire County Council – £100k fine for faxing highly sensitive information to wrong addresses – fax machines no longer to be used?
- A4e - £60k fine for losing unencrypted laptop with personnel information on it

You wish to interview secondary children about their attitudes towards smoking and drugs. What are the data protection issues?
GDPR

- Digital economy and EU harmonisation – effective 25 May 2018

- Evolution not revolution
  - Still only relates to “personal data”
  - Requires closer management of personal data
  - Exceptions for research activities – “research friendly”

GDPR - 7 principles

1. Lawfulness, fairness and transparency (notices, lawful grounds for processing e.g. unambiguous consent)
2. Purpose limitation (stick to purpose)
3. Data minimisation (only take what you need)
4. Accuracy (keep data up to date)
5. Storage limitation (keep only as long as you need the data)
6. Integrity and confidentiality (training, security, “privacy by design”, anonymisation, pseudonymisation, reporting breaches)
7. Accountability (demonstrate compliance)
Recap on the basics

- Consent, anonymise, pseudonymise, minimise
- Keep it safe
  - Local protocol and encryption
- Think before you share
- Privacy impact assessment
- Guidance:
  http://www.leeds.ac.uk/secretariat/data_protection.html
Consent

- Article 6 for non-special category and Article 9 “explicit” for special categories of data

- Consent must be “clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement…” (Recital 32)

- Need consent to **all** purposes (Recital 32)

- Gone are pre-ticked or opt out boxes (Recital 32)

- Must be able to demonstrate consent and language must be “intelligible and easily accessible form, using clear and plain language” (Article 7(2)) with right to withdraw (Article 7(3))
Consent Cont’d

- You are doing research into Government efficiencies and attitudes of Government employees. You have found some extremely useful comments from employees posting on the Twitter website. Comments saying that they think Government is highly inefficient with reflections on their own and Government’s inefficiencies and someone saying they regularly struggle to get into work because of their ‘wine induced hangovers’. Do you need consent?
Consent - breadth

- (Recital 33)
  - Can be to “certain areas of scientific research when in keeping with recognised ethical standards
  - Give opportunity to participate in “certain areas of research or parts of research projects to the extent allowed by intended purpose”
Privacy Notices

- Information/privacy notices = information sheets/consent forms
- General requirement to give notice where directly/indirectly collecting data (Articles 13 and 14)
- Research exemption under Article 14, para 5(b) where “impossible or would involve a disproportionate effort..., subject to Article 89(1) conditions”

Guidance:

Privacy Notice – Direct Collection

- Identity and contact details
- Purpose of processing and legal basis
- Legitimate interest argument
- Recipients of data
- Details of any transfers to third countries and safeguards
- Retention period
Privacy Notice – Direct Collection continued

- Existence of each data subject’s rights
- Any right to withdraw
- Right to lodge a complaint with ICO
- Whether statutory or contractual requirement
- Any automated decision-making
Processing without consent (non-special category data)

- Article 6(1) – six lawful grounds consent only one!
  - 6(1)(e) – “carried out in the public interest”
    - Need to document the public interest ground
  - 6(1)(f) – “legitimate interest” – probably no longer available as University a public authority

Information identifying BNP members without their consent released on to the web. You want to use the data to profile “racism in the regions”. This will be part of a paper that you are paid to deliver at a Government-sponsored conference.
Processing without consent (cont’d)

- Article 9 (special categories of personal data) – 10 lawful grounds
  - 9(2)(a) – “explicit consent” (returned questionnaires?)
  - 9(2)(e) – “personal data...made public by the data subject”
  - 9(2)(g) – “necessary for reasons of substantial public interest”
  - 9(2)(j) – “scientific or historical research purposes or statistical purposes” subject to Article 89(1)
Article 89(1) appropriate safeguards

- Ensure necessary “technical and organisational measures are in place”
  - respect data minimisation
  - apply anonymisation or pseudonymisation where you can
Anonymisation

- Always think about minimisation, anonymisation and security

- Data that is anonymised \textbf{not} personal data as no longer identifiable – Recital 26

- Pure anonymisation difficult
  - “account should be taken of all the means reasonably likely to be used” factors include cost, time and technology
Pseudonymisation

- Article 4(5)
  - Not attributable to individual unless “additional information” e.g. a marker and
  - “additional information” kept secure and separate
- Still personal data
When is the individual identifiable – looking at risk?

- Using identifiers and pseudonymisation
  - ICO “Anonymisation: managing data protection risk code of practice”

- Privacy impact assessments

- Social medial research
Coffee Quiz

- Do you as an individual or your School/research team have to register under the Data Protection Act/GDPR?
- Do you always have to get someone’s consent to use their personal data?
- Three organisations doing research together, what is an acceptable basis for sharing personal data?
- How long can you and should you keep personal data used for research?
- What is the date of birth of Adrian’s Mum?
Collaborative research

- Are you a sole/joint controller or processor?
- Controller, Article 4(7) about determining the “purposes and means of the processing” of the personal data
- Necessary agreements concerning sharing e.g. data processing agreement
Key Concept – Personal Data

- Article 4(1) GDPR *personal data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Sensitive data (DPA 1998) and special categories of data (GDPR)

- Present DPA sensitive data is, information about race, political opinions, religious beliefs or similar beliefs, trade union membership, health, sexual life, offences, criminal proceedings

- Under GDPR special category data (Article 9) excludes the above criminal offences but includes genetic data and biometric data

- Criminal offences separate Article
Individual rights – exemptions available

- Access requests
  - To be free, delivered within one month but
- Rectification (right to have inaccurate personal data rectified)
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Portability (have a copy of personal data held in electronic form)
- Right to object to automated processing
Privacy by design

- Technical and organisational safeguards required
- Build in protection through your systems e.g. minimisation, anonymisation, pseudonymisation, encryption, training and retention schedules
Encryption and passwords

- Recording using encryption
- Using the N drive
- Sending encrypted attachments
  - File, protect, encrypt with password
- Encrypting laptops and other mobile devices
- Good passwords and bad passwords
Breach reporting and impact assessments

- Without undue delay, where feasible report within 72 hours significant breaches to the ICO and affected individuals
- Impact assessments for high risk activities e.g. sensitive or large volumes of data in research
Secondary purpose

- Article 6(1) generally only allows you to process for specified purpose
- Article 6(4) allows you to process for unspecified but “compatible” purpose
- Recital 50 says that processing for research “should be considered to be compatible” but subject to Article 89(1) safeguards
International transfers

- (Article 44) if outside of the EU must have “adequate level of protection”

Useful reference material


https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/


https://www.jisc.ac.uk/events/gdpr-conference-06-dec-2017#resources
GDPR Derogations – Supplemental

• Art. 89(1):
  • Art. 5(1)(b) and (e) – further processing and storage
  • Art. 9(2)(j) – processing of special categories
  • Art. 14(5)(b) – information requirements
  • Art. 17(3)(d) – right to ensure
  • Art. 21(6) – right to object
GDPR Derogations - supplemental continued

- Art.89(2) – Union or Member States can derogate further on subject rights, including:
  - Art. 15 – right to confirmation of processing, access requests and notified safeguards
  - Art. 16 – right to rectification
  - Art. 18 – right to restriction of processing
  - Art. 21 – right to object

- Also requires (1) Art. 89(1), (2) applying the right would render impossible or impair the purpose; (3) the derogations are necessary for the purpose to be achieved
Derogations - Data Protection Bill - supplemental

- Schedule 2, Part 6 section 25 (derogations under Art. 89(2)):
  - Art. 15 right to confirmation of processing, access requests and notified safeguards
  - Art. 16 right to rectification
  - Art. 18 right to restriction of processing
  - Art. 21 right to object to processing.

- Also requires:
  - (1) Art. 89(1)
  - (2) for Arts. 15(1)-(3), the result of the research or any resulting statistics are not made available in a form which identifies a data subject
Handouts
GMC Guidelines on Consent

The information provided should include:

- what the research aims to achieve, an outline of the research method, and confirmation that a research ethics committee has approved the project;
- the legal rights and safeguards provided for participants;
- the reasons that the patient or volunteer has been asked to participate;
- if the project involves randomisation, the nature of the process and reasons for it, and the fact that in double-blind research trials neither the patient nor the treatment team will know whether the patient is receiving the treatment being tested or is in the control group;
- information about possible benefits and risks;
- an explanation of which parts of the treatment are experimental or not fully tested;
- advice that they can withdraw at any time and, where relevant, an assurance that this will not adversely affect their relationship with those providing care;
- an explanation of how personal information will be stored, transmitted and published;
  - what information will be available to the participant about the outcome of the research, and how that information will be presented;
- arrangements for responding to adverse events;
- details of compensation available should participants suffer harm as a result of their participation in the research.
Security Tips

1. Recognise different levels of sensitivity requiring different levels of security
2. Sensitive email attachments to be encrypted
3. No laptops to be taken home with sensitive personal data (what about exam scripts!)
4. Restrict access and get users trained
5. Restrict access to records and prohibit removal from within the School (e.g. health records)
6. Use 7 digit passwords, mix numbers and letters and lower and uppercase if possible
7. Restrict home access to certain areas via the remote server and use Citrix
8. Do not open spam (keep off the porn and don’t respond to the “growth enhancers”)
9. Restriction on printing-off material at home
10. Encrypt databases
11. Use encrypted pen drives:
   1. (AES (Advanced Encryption Standard) 256 Bit Encryption (US Standard);
   2. FIPS 140-2 (UK Government approved standard);
   3. CAPS (CESG Assisted Product Scheme, for commercial off-the-shelf products used by HMG).
12. Always procure that laptops and PCs are wiped when staff leave or equipment about to be “ditched”
13. Shred confidential material
14. Lock away material in cabinets – who’s got the key?
15. Consider impact assessment and doing a local protocol
CONSENT FORM

Please initial the box

1. I confirm that I have read the information sheet.

2. I understand that my participation is voluntary and that I am free to. I will answer all the questions given to me honestly.

3. I understand that once I have given my data it cannot be changed and cannot be deleted.

4. I understand that you will use your reasonable endeavours to preserve my anonymity.

5. Researchers may after speaking to me, breach confidentiality if they reasonably fear there is very serious and imminent danger to myself.

6. I do/do not agree to give a recorded interview.

7. I do/do not agree my words can be deposited in an archive.

8. I acknowledge receipt of £50 by way of compensation for my time.

9. I agree to take part in the research on the above conditions.

.................................................................

Initial of participant

.................................................................  ........................................

Name of person taking consent       Date
Information Protection Policy

Version 1.1 21st June

2013

© University of Leeds 2013

The intellectual property contained within this publication is the property of the University of Leeds.

This publication (including its text and illustrations) is protected by copyright. Any unauthorised projection, editing, copying, reselling, rental or distribution of the whole or part of this publication in whatever form (including electronic and magnetic forms) is prohibited. [Any breach of this prohibition may render you liable to both civil proceedings and criminal penalties].
Document Control

This document is subject to change control and any amendments will be recorded below.

Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Circulation</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>10/03/13</td>
<td><a href="http://www.leeds.ac.uk/informationsecurity">www.leeds.ac.uk/informationsecurity</a></td>
<td>First formal issue</td>
</tr>
<tr>
<td>1.1</td>
<td>21/06/13</td>
<td><a href="http://www.leeds.ac.uk/informationsecurity">www.leeds.ac.uk/informationsecurity</a></td>
<td>1. Added 'unrestricted' to para 5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3. Advice on mobile protection in 12.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4. Safe haven fax added to table.</td>
</tr>
</tbody>
</table>

Version Awareness

The audience of this document should be aware that a printed copy may not be the latest available version. The latest version, which supersedes all previous versions, is available at http://campus.leeds.ac.uk/isms. Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.
Introduction
This policy sets out the steps which members of the University are required to take to protect the security of all ‘sensitive information’, a category which includes but is not confined to information that relates to and identifies individuals (‘personal data’). The policy applies in particular to members of staff, but it also covers students wherever appropriate.

Overview
The Policy classifies sensitive information according to its damage potential, and defines the special controls which are to be applied in order to protect it from inappropriate disclosure. There are two kinds of classified information: ‘confidential’ and ‘highly confidential’.

Any information that is not categorised as either ‘confidential’ or ‘highly confidential’ is ‘unclassified’. No particular controls apply to the disclosure of unclassified material.

- **Highly confidential** applies to information disclosure of which to unauthorised recipients would be likely to result in serious damage to the interests of individuals or of the University.

- **Confidential** applies to information disclosure of which to unauthorised recipients could have a negative impact on individuals or the University.

Except for information which is obviously and legitimately in the public domain (such as job titles and departments), personal data will, as a general rule, fall into one or other of the classified categories.

The scale, volume and the medium of storage need to be taken into account in the assessment of the classification of any set of information. For example, information which in itself would be classified as ‘confidential’ when it relates to just one individual might need to be classified as ‘highly confidential’ when it covers hundreds or thousands of individuals, especially (but not only) if it is held in electronic form. The potential for damage from unauthorised disclosure is very much higher in the latter case than in the former and the level of control needs accordingly to be higher.

Examples of material falling into the above categories are set out in Annex 1.

Requirements
The University is seeking to create and reinforce a culture which takes data security seriously. To this end, all members of the University are expected to comply with the following requirements.

1. Assess the sensitivity of all information you create and receive; and take proportionate measures to ensure that data are held securely. Guidance on whether or not documents should be classified (as ‘confidential’ or ‘highly confidential’), and the key controls for protecting data, are set out in the annexes to this policy. (Further guidance is available at [http://iss.leeds.ac.uk/downloads/download/536/risk assessment](http://iss.leeds.ac.uk/downloads/download/536/risk assessment).)
2. Keep personal passwords secret; never share them. Group passwords must not be disclosed outside the group. (Guidance on passwords is available at http://iss.leeds.ac.uk/info/360/guidelines/774/selecting and protecting your passwords)

3. Access or share classified information only where the conduct of University business requires you to do so and with the necessary permissions.

4. Obtain any necessary permissions before sharing classified information with colleagues or third parties. Seek advice if you are unsure what you need to do (see contact information below).

5. Keep electronic data on the University’s servers. In general, store classified data only on the University’s servers (first encrypting any highly confidential data that is to be kept in unrestricted shared areas). (See also 14 below.)

6. Unless using a bespoke service that has been security-tested and approved by the University, Cloud services must not be used for storing or processing data which is (a) classified; (b) of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted; or (c) valuable intellectual property of the University (on which further advice can be sought from the Legal Adviser).

7. Make sure no one can access your computer when it is left logged on and unattended. Use ‘password protection’ on your computer and on any portable electronic equipment used to store or access University data (including mobile phones used to access e-mail).

8. Comply with the University’s Code of Practice on Data Protection (see http://www.leeds.ac.uk/secretariat/data protection code of practice.html) In particular, anonymise research data wherever possible, only take the data you need; and in any event do not keep data longer than required for the conduct of University business.

9. Never configure your computer (or other hardware) automatically to forward University e-mails to an external service provider (for example, a personal hotmail account).

10. When e-mailing classified information to other members of the University, always use their University e-mail address (rather than externally-hosted e-mail facilities.)

11. When e-mailing data, always double-check that you have used the right address before sending the e-mail. This is particularly necessary when your e-mail system ‘predicts’ the intended recipient from your first few key strokes.

12. When you are off campus, use University-approved methods to access University e-mail or data (such as Outlook Web Access or Citrix for example). If you use mobile devices for this purpose, make sure they are password or pin protected, or otherwise encrypted.

13. Encrypt classified electronic data (a) when holding them on laptops or memory sticks or other removable media and (b) before attaching them to e-mails. Never include ‘highly confidential’ information within the body of an unencrypted e-mail.

14. If you have to keep classified data on laptops, memory sticks and other portable devices, do so only on a temporary basis. Delete such information from the portable device at the earliest possible
opportunity. Keep the volume of data on a memory stick or similar device to the absolute minimum required for immediate operational purposes.

15. Save in very exceptional circumstances, and with the permission of your line manager, highly confidential paper documents should not be taken outside the University; if you have to take classified paper documents outside the University, do so for the shortest time possible, keeping them securely. If you obtain classified information outside the University (for example, through the collection of research data), keep the data securely, and bring or post them into the University at the earliest opportunity.

16. If posting classified material, use a first class envelope for confidential material, and use recorded post and a double envelope (one inside the other) for material that is highly confidential. The external envelope must not bear the classification.

17. Use shredding machines for disposal of classified paper documents. Disposal of bulk classified waste can be carried out through Cleaning Services. Any unwanted, damaged or obsolete computer hardware must be disposed of through Cleaning Services – it cannot be sold or donated to members of the University or to other organisations, such as charities. Seek advice if you are unsure what to do.

18. Ensure offices are locked when they are unattended, and that classified papers are locked away when not in use.

19. Make sure any third parties (including contractors) permitted to handle classified data are required to take appropriate security measures. (A template for use in this connection is available from the Legal Adviser.) Similarly, respect any additional third party rules relating to data that has been shared with the University – for example, by the NHS.

20. If you use a home or other non-University computer to create or access classified information, make sure that the computer has up-to-date security protection, and that no-one else can use it to view University information. Classified data must not be stored on privately-owned computers and equipment.

Overall responsibility for information security issues within the University rests with Roger Gair, the University Secretary. Assistance and training can be provided through Kevin Darley, the University’s IT Security Co-ordinator (k.j.darley@leeds.ac.uk; ☎️ 0113 343 1118) or from Adrian Slater, the University’s Legal Adviser (a.j.slater@leeds.ac.uk).

Any information security incidents or breaches must be reported to one or other of them immediately.

---

1 Examples of cloud services include iCloud, Dropbox, Microsoft (Azure, BPOS and SPLA), Amazon (AWS, S3 and EC2) and Google (Google Apps). Advice on approval of bespoke solutions should be sought from the IT Security Coordinator.

2 This requires the use of the University Encryption Standard. Even those who do not routinely handle classified data may wish to encrypt their laptops. Details are available via the ISS Help Desk.
## ANNEX 1 – Classifying information

### Personal Data

<table>
<thead>
<tr>
<th>Unclassified</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
</table>
| Anonymised data<sup>3</sup>  
Data agreed by data subjects to be put into the public domain.  
Publicly available staff directories including work telephone numbers, e-mail address and Department information.  
Simple list of names with no other data.  
Information on individuals available through social network sites where information provided on condition that will be public domain information. Final degree classification. | Individual’s passport details, home address and telephone number.  
Individual’s name plus home address/postcode, age and home telephone numbers.  
List of student names and their student ID number or list of staff names and their personnel number.  
Names and addresses of student applicants to the University.  
Attendance details relating to an existing student.  
Student transcript  
Exam scripts  
Exam marks  
Examiner’s comments on a student’s performance | Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees).  
Information on individual’s racial or ethnic origin, political opinion, religious or other beliefs, physical or mental health or criminal record.  
Attendance and academic progression information/disciplinary information relating to an existing University student.  
Preliminary degree classification/transcript information pending formal approval and any publication |

### References for students or staff<sup>4</sup>

<table>
<thead>
<tr>
<th>UCAS forms&lt;sup&gt;4&lt;/sup&gt;</th>
</tr>
</thead>
</table>
| Dates of birth.  
Individual’s name plus date of birth or national insurance number<sup>5</sup> | Individual’s name plus date of birth or national insurance number, passport details, home address and telephone number<sup>5</sup>.  
Hundreds of individuals’ names plus date of birth or national insurance number<sup>3</sup> |

---

<sup>3</sup> For these purposes anonymised data is data which does not relate to a living individual and cannot identify an individual, or cannot identify an individual through other information which is in the possession of, or is likely to come into the possession of the organisation processing (see section 1 (1) (a) of the DPA 1998

<sup>4</sup> Content dependent e.g information relating to health, criminal record or disciplinary matters, would make the reference/UCAS form highly confidential.
Adding additional combinations of data can change the overall status. Simply increasing the volume of data can also change status.
### Non-Personal Data

<table>
<thead>
<tr>
<th>Unclassified</th>
<th>Confidential</th>
<th>Highly confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research grant applications/proposals[^6]</td>
<td>Information relating to supply or procurement of goods/services prior to approved publication.</td>
<td></td>
</tr>
<tr>
<td>Information contained within an organisation's annual corporate report.</td>
<td>Assessment material prior to “unseen” assessment</td>
<td>Future marketing or student fees information not yet agreed to be made public. Other information that may be regarded as a trade secret or otherwise highly commercially sensitive.</td>
</tr>
<tr>
<td>Information that can be obtained from publicly available directories or regulatory bodies e.g. Companies House or HEFCE.</td>
<td></td>
<td>Information relating to restricted intellectual property rights or otherwise covered by a confidentiality agreement/ contractual term.</td>
</tr>
<tr>
<td>Information contained within an organisation's web sites for public dissemination.</td>
<td></td>
<td>Legal advice and other information relating to legal action against or by the University.</td>
</tr>
</tbody>
</table>

Please be aware that the above are only indicative general examples of personal and non personal data. As highlighted in the footnotes and main body of the policy, the mix of information, the amount of information and the medium in which the information is held can change the classifications.

[^6]: Content dependent e.g. information subject to imminent academic publication or industrial collaborators may lead to application/proposal being highly confidential.
## ANNEX 2: Key controls for protecting classified information

<table>
<thead>
<tr>
<th>Activity</th>
<th>Confidential</th>
<th>Highly Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electronic data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage of data in <em>shared</em> areas of University server</td>
<td>Yes</td>
<td>Only if encrypted</td>
</tr>
<tr>
<td>Storage of data in personal area of University server</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote access to the data</td>
<td>Yes, but only via Citrix or other University-approved mechanism</td>
<td>Yes, but only via Citrix or other University-approved mechanism</td>
</tr>
<tr>
<td>Storage of data on University-owned laptops or other portable devices.</td>
<td>Only on a temporary basis and only if encrypted</td>
<td>Only on a temporary basis and only if encrypted</td>
</tr>
<tr>
<td>Storage of data on privately-owned laptops or other portable devices (including memory sticks)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sending data by e-mail</td>
<td>Yes (taking care to check the address of the recipient(s))</td>
<td>Yes but only as encrypted attachment</td>
</tr>
<tr>
<td><strong>Paper and other media</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage in University</td>
<td>Locked filing cabinet or equivalent</td>
<td>Locked filing cabinet or equivalent inside room normally kept locked</td>
</tr>
<tr>
<td>Facsimile transmission</td>
<td>Yes</td>
<td>No (unless directed to a ‘safe haven’ machine)</td>
</tr>
<tr>
<td>Data collection outside the University</td>
<td>Kept securely on the person (and returned to the University at the earliest opportunity)</td>
<td>Kept securely on the person, preferably in a locked case (and returned to the University at the earliest opportunity)</td>
</tr>
<tr>
<td>Taking documents off campus</td>
<td>For the shortest time possible and documents to be kept securely about the person</td>
<td>Only permitted exceptionally and once authorised by your line manager</td>
</tr>
<tr>
<td>Posted</td>
<td>Yes via first class post in an envelope without any classification marking</td>
<td>Yes, via Recorded post when double enveloped, without classification marking on outer</td>
</tr>
<tr>
<td>Disposal</td>
<td>Shred small volumes. Bulk disposal through cleaning services.</td>
<td>Shred small volumes. Bulk disposal through cleaning services.</td>
</tr>
</tbody>
</table>
Remote access to unencrypted information is possible only to information in the personal area of a server.

Recorded post requires a signature from the recipient; other forms of post requiring a signature (e.g. Special Delivery) are also legitimate.
Adrian's sensitive data practice – not “Perfect Peter”!

1. Always doublecheck predicted e-mail addresses.
2. Always lock my office when unattended.
3. Rarely take home highly confidential paper documents. If I do, only keep overnight and always keep about me and locked up.
4. Any electronic personal data taken home on encrypted pen drive.
5. Encrypt attachments when sending e-mails outside of the University that are highly confidential.
6. Generally do not use Wi-Fi outside of the University on my iPhone. Keep iPhone password protected.
7. Use Citrix when accessing work PC from home. Got home security software running.
8. The box next to my desk for shredding confidential material.
9. Put nothing confidential in the green bins or other bins.
10. Double sweep of meeting table when leaving a meeting.
11. Always save documents onto the central drive. Sometimes save documents into personal area only.
12. Only put lecture handouts/PowerPoints onto unencrypted memory stick.
13. I don't use my laptop as not encrypted.
15. I do not share my password with anyone.
16. Carry confidential paper documents around the University in a file or clipboard folder.
17. I don't search "shady" websites or respond to unknown e-mails at work (not even at home actually, honestly!).
DISCLOSURE AGREEMENT

THIS AGREEMENT is made on January 2012

BETWEEN:

(1) University of Leeds, Leeds LS2 9JT, United Kingdom (“Discloser”);

and

(2) [ ] (“Recipient”)

BACKGROUND

[ ]

NOW IT IS HEREBY AGREED as follows:-

1 DEFINITIONS

In this Agreement unless the context otherwise requires:-

1.1 “Confidential Personal Data” means [ ] [all information which is disclosed by the Discloser to the Recipient for the achievement of the Purpose and which constitutes personal data as defined by the Data Protection Act 1998].

1.2 “Purpose” means [ ].

2 OBLIGATIONS OF THE RECIPIENT

2.1 In consideration of the disclosure of the Confidential Personal Data, the Recipients undertake:

(a) to use the Confidential Personal Data for the Purpose only and for no other purpose;

(b) not to disclose the Confidential Personal Data to any employees who have no direct involvement with the Purpose;

(c) not to disclose the Confidential Personal Data to any third parties;
(d) to keep the Confidential Personal Data secure and in particular [ ];
(e) [to ensure that the published Project Report does not contain Confidential Personal Data unless the express and prior written consent of the Discloser has been granted;]
[to not publish any of the Confidential Personal Data without the Discloser's written consent;]
(f) to return all Confidential Personal Data (including any copies made thereof) to the Discloser immediately on completion of the Purpose and to certify in writing to the Discloser that this obligation has been fully discharged.

3 EXCLUSION AND ENTIRETY

3.1 The Recipient shall use the Confidential Personal Data entirely at its own risk. The Discloser offers no warranty as to the accuracy or completeness of the Confidential Personal Data. Save where the negligence of the Discloser shall cause death or personal injury all liability of the Discloser is excluded.

3.2 This Agreement constitutes the entire understanding between the parties relating to the release of the Confidential Personal Data.

Agreed on the date above
Signed by
DATA SHARING AGREEMENT

PARTY A

and

THE UNIVERSITY OF LEEDS
AGREEMENT DATED [insert date]

BETWEEN:

(1) [PARTY A] (“[Party A]”); and

(2) THE UNIVERSITY OF LEEDS having its main address at Leeds, LS2 9JT (the "University").

BACKGROUND

(A) This Agreement is to ensure there is in place proper arrangements relating to personal data passed from Party A to the University.

(B) Taking into account standard written guidance offered by the Information Commissioner’s Office [link], it has been agreed that each of the parties is a data controller in relation to the data being transferred under this Agreement.

(C) This Agreement has been written reflecting requirements under the ICO’s “Data sharing code of practice”.

(D) The parties wish to record their commitment to sharing arrangement under the terms of this Agreement.

IT IS AGREED AS FOLLOWS:

1. **Definitions and Interpretation**

   In this Agreement:

   "Data Protection Laws" means the Data Protection Act 1998, together with successor legislation incorporating GDPR;

   "Data" means personal data passed under this Agreement, being in particular the type of data to be shared as detailed under the Table;

   “Data Subjects” means the individuals identified by the Data;
“GDPR” means the General Data Protection Regulation;

“Purpose” means the activity to be completed by Party A as described under the Table;

“Table” means the table detailed under Part C of the Annex.

2. **Purpose of Sharing**

2.1. The parties agree to share the Data transferring from Party A to the University to achieve the Purpose, and only for the Purpose.

3. **Organisations Involved in The Sharing Of The Data**

3.1. The Table contains details of any third parties who may be given access to the Data and on what basis. No additional parties may process the Data without the written consent of Party A.

4. **Data Items To Be Shared**

4.1. The description of the Data under the Table gives a detailed explanation of the Data to be shared.

5. **Basis for Sharing of the Data**

5.1. Each of the parties has obtained the consent of the Data Subjects to sharing of the Data.

5.2. Data Subjects have been given the right to withdraw their consent. If either party receives such a request they shall immediately pass on the request to the other party so that the Data Subjects’ Data can be deleted.
6. **Access and Individual Rights**

6.1. It is recognised that Data Subjects have rights under Data Protection Laws. If at any time a Data Subject shall seek to engage any of these rights that also requires action by the other party then the party receiving notice from the Data Subject shall also inform the other party. The other party shall respect the rights of the Data Subject and take action as required.

7. **Information Governance**

7.1. Parties have carefully considered the minimum amount of data that may be shared in order to fill the Purpose. The Data reflects this minimum amount.

7.2. In order to ensure that the Data being shared is accurate [*describe any action taken to ensure updates etc included*].

7.3. [*Statement about how we will ensure the two sets of data (existing and shared) are compatible if relevant e.g. by use of identifiers such as dates of births and names.*]

7.4. Agreed periods of retention for the Data are specified under the Table.

7.5. The agreed technical and organisational security arrangements relating to the transmission and storage of the Data are described under Part A of the Annex.

7.6. Any requests from Data Subjects for exercising their rights under Data Protection Laws or the Freedom of Information Act (including complaints or queries) will be dealt with through the representatives described under Part B of the Annex.

7.7. The parties shall every [12 months] review this Agreement to ensure that it remains fit for purpose in achieving a safe sharing of Data between the parties respecting the rights of the Data Subjects.

8. **Co-operation**

8.1. Each party agrees to provide the other with all information necessary to demonstrate compliance with the obligations laid down under this Agreement and for the completion
of any reasonable audit, inspection or verification to ensure that the rights of Data Subjects are being respected.

9. Transfer of Data

9.1. Arrangements relating to the secure transfer of the Data between the parties are detailed under the Table.

10. Integrity of the Data

10.1. [What can we say about keeping the integrity of the data?]

11. Data Breach

11.1. Each party shall immediately contact the other through the representatives described under Part B of the Annex if there is any breach of security or incident relating to the Data where the Data may have been compromised.

12. Termination

12.1. A party may immediately terminate this Agreement if the other shall be in material breach of its terms and not remedied the breach within a period of 30 days.

13. General

13.1. This Agreement may only be varied with the written consent of both parties.

13.2. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex.

13.3. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller relationship under Data Protection Laws.

13.4. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts.

For and on behalf of The University of Leeds
For and on behalf of Party A
ANNEX

Part A

Security of Processing

1. Consideration of anonymisation, pseudonymisation and encryption.
   [The Data will be encrypted and saved in a password protected folder on the University’s secure server.]
   Access within the University’s organisation will be limited to [ ].
   No Data will be held on laptops or other external storage devices.]
   [Anonymization and pseudonymisation of the Data has been considered but is not practical given the need to update Data against identified individuals]

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related Purpose.
   [Ongoing confidentiality and integrity of data is assured by account access controls and restricted permissions. Data availability is assured through asynchronous replication of data to an off-site location. Processing systems are protected through firewalls, intrusion prevention systems and machine room environmental controls, such as UPS, and water and fire detection / suppression.]

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
   [The Data will be hosted on the University’s file share which is regarded as a crucial system for the University’s operations. As such recovery of this would be a high priority in the event of a physical or technical incident. In the worst case scenario the last 4 hours of Data would be lost as the asynchronous replication process to off-site systems takes place every 4 hours.]

4. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.
   [The University has deployed a Security Incident Event Management (SIEM) system to monitor critical systems and carries out regular vulnerability assessments along with internal and external penetration testing as and when required]

5. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.
   [Please see the Table for description of method of data sharing.]

6. The University to ensure that anyone acting on their behalf does not process any of the Data unless following instructions from Party A unless they are required to do so under English law.
ANNEX
Part B

Party A Representative shall be [ ]

The University Representative shall be [ ].
<table>
<thead>
<tr>
<th>The Purpose</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Method of data sharing</td>
<td></td>
</tr>
<tr>
<td>Format of Data</td>
<td></td>
</tr>
<tr>
<td>Third parties with access to the Data</td>
<td></td>
</tr>
<tr>
<td>Data retention period</td>
<td>Data will be retained until</td>
</tr>
<tr>
<td>Data storage</td>
<td>See Part A.</td>
</tr>
</tbody>
</table>
DATA PROCESSING AGREEMENT

THE UNIVERSITY OF LEEDS

and

[ ]
AGREEMENT DATED [insert date]

BETWEEN:

(1) THE UNIVERSITY OF LEEDS of Leeds LS2 9JT ("Leeds"); and
(2) [              ], having its registered office at [              ] (the "Processor").

BACKGROUND

(A) This Agreement is to ensure there is in place proper arrangements relating to personal data passed from Leeds to the Processor.
(B) This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation.
(C) The parties wish to record their commitments under this Agreement.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

In this Agreement:

"Data Protection Laws" means the Data Protection Act 1998, together with successor legislation incorporating GDPR;

"Data" means personal data passed under this Agreement, being in particular [describe personal data being passed];

"GDPR" means the General Data Protection Regulation;

"Services" means [describe the services provided by the Processor to Leeds].

2. DATA PROCESSING

Leeds is the data controller for the Data and the Processor is the data processor for the Data. The Data Processor agrees to process the Data only in accordance with Data Protection Laws and in particular on the following conditions:

a. the Processor shall only process the Data (i) on the written instructions from Leeds (ii) only process the Data for completing the Services and (iii) only process the Data in the UK with no transfer of the Data outside of the UK (Article 28, para 3(a) GDPR);

b. ensure that all employees and other representatives accessing the Data are (i) aware of the terms of this Agreement and (ii) have received comprehensive training on Data Protection Laws and related good practice, and (iii) are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR);

c. Leeds and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement (Article 28, para 3(c) GDPR);

d. the Processor shall not involve any third party in the processing of the Data without the consent of Leeds. Such consent may be withheld without reason. If consent is given a further processing agreement will be required (Article 28, para 3(d) GDPR);
e. taking into account the nature of the processing, assist Leeds by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of Leeds’ obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making etc (Article 28, para 3(e) GDPR);

f. assist Leeds in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO etc, taking into account the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR);

g. at Leeds’ choice safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services]. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the Data. Where there is a legal requirement the Processor will prior to entering into this Agreement confirm such an obligation in writing to Leeds. Upon request by Leeds the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR);

h. make immediately available to Leeds all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by Leeds from time to time (Article 28, para 3(h) GDPR);

i. arrangements relating to the secure transfer of the Data from Leeds to the Processor and the safe keeping of the Data by the Processor are detailed under Part A of the Annex.

j. maintain the integrity of the Data, without alteration, ensuring that the Data can be separated from any other information created; and

k. immediately contact Leeds if there is any personal data breach or incident where the Data may have been compromised.

3. **Termination**

Leeds may immediately terminate this Agreement on written notice to the Processor. The Processor may not terminate this Agreement without the written consent of Leeds.

4. **General**

a. This Agreement may only be varied with the written consent of both parties.

b. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex.

c. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under Data Protection Laws.

d. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts.

For and on behalf of The University of Leeds
For and on behalf of [ ]
ANNEX

Part A

Compliance with Article 32, para 1 of GDPR

7. Consideration of anonymisation, pseudonymisation and encryption.

   *Is the above possible? If not, please explain why. If possible please insert details.*

8. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services.

   *Please explain how the above will be delivered.*

9. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

   *Please confirm the above is possible and description of process in place to deliver the above.*

10. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.

    *Please confirm the above process is in place and broadly what that process is.*

Compliance with Article 32, para 2 of GDPR

11. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

    *Please describe secure transfer process from Leeds to the Processor and levels of security to be applied by the Processor when the Data is in their possession.*

Compliance with Article 32, para 3 of GDPR

12. Adherence to an approved code of conduct referred to in Article 40 (GDPR) or an approved certification mechanism as referred to in Article 42 (GDPR) may be used as an element by which to demonstrate compliance with the requirements set out in para 1 of GDPR – see above.

    *Please describe any relevant code of practice relied upon.*

Compliance with Article 32, para 4 of GDPR

13. The Processor to ensure that anyone acting on their behalf does not process any of the Data unless following instructions from Leeds unless they are required to do so under English law.
ANNEX

Part B

Leeds Representative shall be [insert details] or such other person as shall be notified by Leeds [insert details].

The Processor Representative shall be [insert details] or such other person as shall be notified by the Processor [insert details].