Data Protection

(This chapter contains relevant sections from Northumbria's Data Protection *Policy and Records Management Framework. The* ***UK Data Protection Act 1998*** *will be replaced by the* ***General Data Protection Regulations*** *on* ***25th May 2018****. Updates reflecting the changes to the law will be made to this section during the course of the 2017/18 Academic Year. As a result, it is advised that you monitor the web version of this handbook and do not rely on printed versions. Any queries should be directed to Northumbria's Records and Information Manager, Duncan James).*

It is the duty of all staff and students undertaking research activities to follow and maintain the highest standards of academic practice when processing information about living individuals (personal data) as part of their research. All processing of personal data must be in compliance with the terms of the Data Protection Act (1998) (hereafter referred to as 'the Act').

The level of impact the Act will have upon a research project will be determined by such factors as the method in which personal data is collected, the content of the information and whether an individual can be identified by it. It also affects how the results of the research can be published when looking at whether or not the output contains anonymised or identifiable information.

Whilst this guide provides general practices to be followed at Northumbria University, research projects sponsored by external funders may be required to follow specific procedures as dictated by the funding body (the full policy contains relevant extracts from a number of funders).

The main principles of the Act affecting researchers are that personal data should only be collected, recorded and processed:

- with the express permission of the individual to which it relates
- for the purposes for which the person gave their permission
- and retained for as long as necessary to execute that purpose.

Data Controllers, Data Processors and Student Research

Data Controllers
A Data Controller is the person (or organisation) who determines the purpose for which personal data is to be processed and is responsible for ensuring that processing is 'fair and legal'. The data controller is responsible for instructing a data processor on their requirements for processing personal data and must ensure that the processor conforms to these.

The data controller for research will be determined by who the lead organisation is for the research project,

- Northumbria University will be the data controller where the University is the project lead
- There might be joint data controllers where Northumbria University is in equal partnership in leading a project.
- Research funded by and/or undertaken on behalf of a third party will usually identify the third party as the data controller, unless otherwise agreed.

Data Processors
A data processor is an organisation that processes data on behalf of a data controller and therefore must do so in line with the requirements of the data controller at all times.

- Where partner institutes are contributing to a Northumbria University led project, they are the data processor on behalf of Northumbria University.
- Where research is funded by a third party or the project is led by a third party, Northumbria University is usually the data processor.

Student Research

Students participating on a Northumbria University or third party led projects will be data processors on behalf of the project lead.
Students who undertake their own research requiring the collection of personal data do so because they have determined that they need to collect that data, they have identified what data they need and they have determined how it should be collected (even if they are following recommendations made by their supervisors). Students are therefore the data controller for their own individual research. The University is responsible for ensuring that students are adequately advised and guided on data protection issues and anyone processing personal data should be aware of the following issues.

Using Anonymised Data

Anonymised data exists when it can no longer be used to identify a living individual either by itself or in conjunction with any other information available to the person possessing that data.

An example of this would be where a researcher creates two lists to manage the 'anonymity' of the data subjects.

- The first list, the "index list," contains a unique reference number next to the names of the participants.
- The second list, the "working list," uses the same reference numbers against each set of data collected.

By themselves, neither list identifies a specific individual, even though they both contain 'personal information' and it is not until they are together and the reference is used that they identify each individual and the details they have submitted.

In this situation, it is important to store the two lists separately so the list containing the names would be locked away from the "working" list.

Data which is truly anonymised and cannot be used to identify a living individual is not affected by the DPA. However, this does not mean that data should be anonymised 'for the sake of it' or that you should dispose of the 'index list' just to forgo data protection responsibilities. The index list is still an important project record and must therefore be retained for as long as the information contained within it still has a legitimate purpose, for example should proof be required that people used in the research were genuine.

Using Personal Data

The use of personal data for research should be limited to include only that information which is legitimately and exclusively required to complete the task for which it is deemed necessary. This requires researchers to clearly define exactly what personal information they require and for what purpose it is to be used, before they begin collecting and processing it. They should not collect any additional information that is not relevant to the project in hand. For example, if their research requires them to compile data relating to someone's race or sexuality, they should clearly state why the information is required. If there is no just reason to collect such information they should not do so.

The Requirement for Consent

The Act states that the processing of personal data should normally only take place where the living individual to whom the data relates has 'freely given' their consent for it to be used having been 'fully informed' (see 'Obtaining Consent', below) as to how the information will be used. This information should be supplied to the data subject in the form of a "fair processing notice" (see below).

Researchers are afforded some exemptions from obtaining consent where they can prove that (within the law) there is substantial public interest in processing the information without first obtaining consent or where it is not possible to obtain consent *and* its use is 'fair and ethical' so that it does not result in the unwarranted prejudice to the rights, freedoms or interests of the data subject. Applying 'substantial

public interest' can be difficult, so it is important to back up its application by including a statement in the project documentation indicating the potential benefits to the public of the research. Approval should also be sought from the University Research Ethics Committee.

Examples of personal data processed without the explicit consent of the data subject include:

- where the information has been collected for a previous research project and the new project is a continuation of or is related to that project. In this situation, consent should be obtained from the original researcher(s) to use the data.
- where the information is already in the public domain and the use of such data is not likely to cause unwarranted prejudice to the rights, freedoms or interests of the data subject.

Examples of **sensitive personal data** processed without the explicit consent of the data subject include:

- medical research carried out by a health professional or by someone with a similar duty of confidentiality;
- analysis of racial/ethnic origins carried out for equal opportunities monitoring

Advice on whether or not consent is required to process personal data can be provided by the University Records and Information Manager.

Obtaining Consent

'Freely given' and 'fully informed' consent means that the individual gives consent without any undue pressure from the researcher and with full knowledge and understanding. Consent can subsequently be withdrawn.

An individual may agree to provide personal details in order to answer a researcher's questions, but this does not automatically mean that they are happy to have their details published. Similarly, an individual may be happy for their information to be held and used by the University, but may object if they discover the research is being conducted by the University but on behalf of another organisation. This means that it is important to inform them of all aspects of the research project that may affect them.

Who Gives Consent?

Adults
When collecting information from participants over the age of 18, it should, in most cases, be possible to obtain consent from the individual to whom the data relates. Consent should not be obtained from anyone else (wife, husband, partner, etc.) if the adult is capable of providing it.

Adults Lacking the Capacity to Consent
It should be assumed that subjects will have the capacity to consent in the first instance. All practical and appropriate steps to enable them to make the decision to participate in your research must be taken.

Before deciding that someone lacks capacity to make a particular decision, certain steps are set out in the Mental Capacity Act 2005 (if the research is taking place in England or Wales) or in the Adults with Incapacity (Scotland) Act 2000 (if the research is taking place in Scotland). See page 5 for more details.

Clear guidance is provided in the Code of Practice for the Act and must be adhered to. A helpsheet for social scientists, which is applicable to other disciplines too, and which provides helpful definitions of some of the Act's terms, advice and case examples.

If the project does involve collecting information from individuals who are deemed incapable of

understanding what is being asked of them or making their own decision to take part (i.e. lacking capacity to give informed consent), it is a legal requirement that explicit approval must be obtained from a research ethics committee (REC) that is recognised as an 'appropriate body' under the MCA; currently only NHS RECs and the Social Care REC, all of which work to the standards of the Health Research Authority service, possess that recognition. In order to obtain approval, you must be able to demonstrate that you have an understanding of the legal responsibilities placed upon researchers under the Act. Note that these requirements apply:

- to intrusive research, which is defined as any research which would require the participant to give informed consent
- irrespective of the research discipline; for example, such widely varying research studies exploring the development of assistive technology, or art therapy, in residential care homes which included people with dementia, would fall within the provisions of the MCA.

Applications for approval are made through the Integrated Research Application System (IRAS) after obtaining Northumbria Internal Approval for IRAS here.

Persons under the age of 18
The Act states that collecting personal information from anyone under the age of 18[3] does not always require the consent of parents or guardians if the child is deemed capable of understanding fully what is being asked of them.

There is no set age under the Act as to when someone is 'old enough to understand' so this may need to be assessed on a case by case basis. When someone is deemed old enough to understand what is being asked of them and provide their own consent, parents or guardians are not authorised to give it on their behalf. Where they are not capable of giving consent themselves, parents or guardians must be consulted.

Projects which require the collection of data from persons who are under 18 without the parents' permission or knowledge should make this clear in their proposal when it is submitted to the Ethics Committee - data collection should not proceed without the Committee's approval.

If you are working with persons under 18 in the UK (age limit may differ in other parts of the world), and usually with vulnerable adults, you must have Disclosure & Barring Service (DBS) clearance. DBS replaces the Criminal Records Bureau Check. Refer to Chapter 5 for more information.

Individuals have been screened by means of a certificate (previously known as a 'Disclosure') obtained from the DBS. A Disclosure is an impartial and confidential document that details an individual's criminal record and where appropriate, details of those who are banned from working with children. The DBS will carry out a criminal record check for an individual drawing on four primary sources of information:

- Police National Computer (PNC)
- Local Police Force Records
- Department of Health
- Department for Education and Skills

According to the nature of the contact requirements, information will be drawn from the PNC alone or from every source. This defines 'Disclosure' and constitutes a national standard throughout England and Wales.

Further information about Disclosure is available on the University Website here.

Please see also the University's Policy on Research involving Children and/or Vulnerable Adults.

New Requirements under GDPR

Transparency

Under the new General Data Protection Regulations, which come into force on 25th May 2018, all researchers undertaking research involving personal data must provide information to subjects about the collection and processing of their data.

Remember: where participant data is no longer identifiable, then it is no longer personal data, and the GDPR transparency requirements do not apply.

Under GDPR researchers will now need to provide transparency information about the legal basis for undertaking research and other details of data processing. The table below (Fig 1) sets out the required information that researchers will need to provide when collecting personal data from 25th May 2018.

[3] As a rule, Northumbria University states that collecting personal data from anyone under 18 should only be done with the permission of the individual's parents. However, the University recognises that it is not always possible to conduct research with youngsters where they may not wish their parents to know that are taking part (for example, projects involving underage smokers).

Appendix 1 – transparency requirements

	Personal data obtained directly from participants	Personal data obtained indirectly
Name of controller and contact details (including of data protection officer)	✓	✓
Purposes of the processing, as well as the legal basis	✓	✓
The categories of personal data concerned		✓
The recipients or categories of recipients of the personal data, if any	✓	✓
The period for which the personal data will be stored	✓	✓
The data subject's rights[2]	✓	✓
The right to lodge a complaint with the ICO	✓	✓
The source from which the personal data originate, and if applicable, whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
Any automated decision-making, and, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject	✓	✓
How appropriate or suitable safeguards are achieved in relation to any personal data transferred out of Europe	✓	✓

Fig 1

If your study has already collected personal data at 25th May 2018, the NHS HRA guidance advises that you will not need to provide new transparency information under GDPR, even if you have yet to analyse that data. If the study will be collecting additional personal data after 25th May 2018 or if you're starting a new study after this date, then you will need to provide new transparency information to

participants. This will be either via a separate document notified to participants or by updating the Participant Information Sheet.

Parts of the new GDPR transparency requirements will be familiar to researchers - some of it is the type of information already included on a participant information sheet. However, other elements in Fig 1 will be unfamiliar. The most significant of these is the need to provide the "legal basis" for processing the personal data. It is important to note that, although you will still be required to obtain consent from data subjects in most cases, consent ***will not*** usually be the legal basis for processing data for research purposes in a university context. In most cases of university research, the legal basis will be:

Article 6(1)
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested the controller;

Both the ICO and the Explanatory Note to the Data Protection Bill state that research in universities should be able to rely on this lawful basis.

Where research uses special categories of personal data (e.g. racial or ethnic origin, political opinions, religious beliefs, sexual orientation etc.) then an additional legal basis is required. One of these is specifically directed towards research, so in most cases researchers should use the following as the legal basis for processing special categories of personal data:

> *Article 9(2)(j)*
> *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

Researchers will need to ensure that appropriate safeguards are in place to rely on this legal basis (see below).

In order to communicate this transparency information to research participants, current best practice suggests a "layered" approach - for example, using a Participant Information Sheet to communicate the basics, and then pointing to further resources (e.g. research project webpages) where further detail can be provided. The guidance for preparing a Participant Information Sheet has been updated with some suggested wording to enable researchers to comply with GDPR.

Safeguards

There is a greater emphasis under GPDR on implementing safeguards for research data management. This will mean researchers should carefully consider arrangements for security and storage of data, anonymise or pseudonymise data where possible, and that personal data are only collected when needed to undertake the research ('data minimisation').

> In particular, where research involves processing of special categories of personal data additional measures must be in place to safeguards the rights and interests of the data subject. MRC guidance advises that typical research governance arrangements such as ethical review, peer review from public funders, data minimisation, pseudonymisation and other technical safeguards (such as secure storage, regular backups, clear onboarding and offboarding processes for project staff accessing electronic files, etc.) will be sufficient to meet this criterion.

Help and support

Apart from the guidance in this section of the Handbook, there is revised guidance available for preparing a Participant Information Sheet on the Ethics and Governance webpage (under

'documentation and guidance), GDPR training for researchers and there is further GDPR information available on the University intranet

For further advice on any of these issues, please contact the University's Data Protection Officer: dp.officer@northumbria.ac.uk

Privacy Information Notices under GDPR

Under GDPR data subjects must be given privacy information on how their data is going to be collected and processed. For research projects, this is a familiar requirement: researchers following good research practice are already expected to explain clearly to participants the aims of the research project they have been asked to take part in and state the manner in which the information they supply is to be used. This would typically be communicated using a Participant Information Sheet or similar tool.

The Information Commissioner's Office indicates that there is discretion for data controllers to consider displaying information required by GDPR in different "layers" of a notice - for example, including basic information in a Participant Information Sheet and more detailed descriptions in a project website or in other supplementary information[4]. While including all of the below in a Participant Information Sheet would technically meet the requirements of GDPR it may not be the best way to communicate this information to your research participants. Good research practice should consider the needs and communication preferences of participants and act accordingly.[5]

[4] See: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[5] For health related research, the HRA has published recommended wording for Participant Information Sheets: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data- protection-and- informationgovernance/gdpr-guidance/templates/transparency-wording-public-sector/.

As indicated in Fig 1 above, GDPR requires more detailed information to be provided to data subjects than was the case under the Data Protection Act (1998). What you must tell the data subject also depends on whether the personal data is being obtained *directly* from participants or *indirectly* (see Fig 1):

Name of controller and contact details (including of the organisation's data protection officer): This will usually include:

- The name of the lead researcher (student or member of staff) conducting the research where they are data controller;
- Northumbria University for research projects where the University is the lead - and details of our DPO available here: https://www.northumbria.ac.uk/about-us/leadership-governance/vicechancellors-office/legal-services-team/northumbria-data-protection/ico-notification/ or email: dp.officer@northumbria.ac.uk;
- The name of the project funder;
- In some cases it may be prudent to include that data is being collected by Northumbria University on behalf of x (where x is the name of the funding organisation) and the contact details for both organisations.

Purposes of the processing, as well as the legal basis: This should be a brief but clear description of the project's aims and objectives so that the individual can decide if it is something they are happy to support.

As discussed above, in the New Requirements Under GDPR section, the legal basis for university research projects will in most cases be Article 6(1) (e)..... "task in the public interest".

If the research is collecting special categories of personal data (e.g. racial or ethnic origin, political opinions, religious beliefs, sexual orientation, etc.) then an additional legal basis is required and must be communicated to the data subject. Again, in most cases researchers should rely on Article 9 (2)(j) "processing necessary for scientific and historical research purposes".

The categories of personal data concerned: Required if personal data is to be obtained indirectly. For example this might be contact details, financial information, biometric or health data, depending on the nature of the research.

The recipients or categories of recipients of the personal data, if any: Who is going to be using the personal data, apart from the research team? For example, will the research involve transferring personally identifiable data to third parties for further processing? This may be research teams in other universities, or it may be the funder or other agencies.

The period for which the personal data will be stored: This should be as little as possible, as per the principles of 'data minimisation'. The University has retention schedules[6] for different categories of data, and you should follow these as a basis, unless the funder stipulates a different period of retention. Though a funder may expect data to be retained for a longer period, and in many cases made accessible on a data repository, this will almost always be anonymised data rather than personally identifiable data. If the data has been properly anonymised, then it is no longer personally identifiable data and therefore no longer subject to GDPR.

The data subject's rights: A statement outlining the individual's rights under GDPR should be included[7], including the following: a right of access to a copy of the information comprised in their personal data (to do so individuals should submit a Subject Access Request); a right in certain circumstances to have inaccurate personal data rectified; and a right to object to decisions being taken by automated means. It should be noted that some of these rights are subject to derogations for research-related activity[8]. For example, where giving access to data or rectifying data may "render impossible or seriously impair" the scientific research, then it may be possible to refuse to comply with these rights. However, this would be considered on a case by case basis in close liaison with the University's Data Protection Officer.

The right to lodge a complaint with the Information Commissioner's Office: Simply inform the participant that if they are dissatisfied with the University's processing of your personal data, they have the right to complain to the Information Commissioner's Office. For more information see Information Commissioner's web site.

[6] https://www.northumbria.ac.uk/about-us/leadership-governance/vice-chancellors-office/legal-services-team/records-management/

[7] https://ico.org.uk/

[8] See Article 89 (2) in the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Automated Decision Making: 'Automated decisions' occur where systems make decisions about a person 'automatically' without human intervention. If this is a feature of the proposed research, then you should provide details here and notify the data subject that they have a right to seek human intervention by contacting the lead researcher (give name and contact details).

Appropriate and suitable safeguards for transfer to third party countries: Where personally identifiable data is required to be shared with third parties based either within or outside the EU, then you should ensure appropriate safeguards are in place for this sharing and communicate these to the data subjects. See above section for more on safeguards.

Recording Consent

Recording consent provided by an individual will also be dependent upon the media by which the data is being collected.

Web based collection may be recorded by (but not limited to) methods such as ticking an acceptance box before clicking 'submit,' or by emailing their acceptance. Telephone or other oral methods of collection may involve the data subject speaking their consent onto a recording.

Written consent can be recorded using a signed consent form and stored securely by the researcher along with other project documentation. Examples and template consent forms can be found here under

the heading 'Documentation and Guidance'. Explicit consent must be established when dealing with sensitive personal data.

Disclosure of Personal Data

Personal data must not be disclosed to any third party individual without the consent of the individual. A third party is anyone who is not the data subject or those permitted to process the data. Only the researcher(s) working with the data should be accessing it.

Individuals who provide personal data may at a later date ask an organisation for access to the information they have provided. In order to do this, they must submit a 'subject access request' to the University. The University will then have 40 days to provide the information.

Individuals also have the right to withdraw their consent to the University processing their personal data. If consent is withdrawn, processing must stop within 15 days of the withdrawal and confirmation that this is the case should be sent to them.

Publishing Personal Data

If the research requires the publication of personal data, this must be done in accordance with the method described when consent was provided by the individuals. For example, if consent was provided on the basis that personal data would be anonymised or that it would not be published on the internet, neither is permitted. Because of this, it is important to provide data subjects with comprehensive information when they are deciding whether or not to provide consent.

Internet Based Research

Internet based research (often referred to as Internet-Mediated Research) is an ever-changing means of conducting research through existing and emerging web based technologies, each with their own unique advantages and disadvantages. Internet research may range from simple online surveys delivered via platforms such as the onlinesurveys provided by JISC (previously the Bristol Online Survey system), to in-depth and large scale data mining of material already posted online across blogs, discussion fora or social media sites, or through inviting proactive participation through such sites. For students/staff that would like to make use of BOS service, they could contact it.helpline@northumbria.ac.uk to join the Northumbria University online surveys account.

Because researchers and participants rarely meet face to face when conducting internet based research, it is often to gauge where individuals are giving free and informed consent to take part in research. Consideration must always be given to how to establish the participants are old enough, competent enough to freely give their own consent (i.e. someone isn't giving it on their behalf).

Things to consider when utilising online research include:

Selecting the Platform
Researchers inviting participants to partake in their online research have an obligation to ensure that the platform they are using is appropriate and adequately secure enough to ensure that the privacy rights of the participants are met. When selecting the platform, researchers should consider, but not limited to, the following:

- The sensitivity of the data they are collecting – higher risk means more secure!
- The nature of their research and what method of collection is appropriate – survey or social media?
    - Where is the system hosted? USA takes personal data beyond the European Economic Area and may therefore breach the Data Protection Act.
    - How long the system stores data for – can data be will deleted it at the end of a project or is it archived on a server somewhere?
    - Will participants need to log in and if so, how?

- Can individual requests to delete data be processed?
- How will the processing notification be published?
- Does the system have the capability to record the correct level ofconsent?

Recruitment
The lack of face to face meeting between researcher and participant can create issues with the recruitment and verification of the identity of participants. In low risk research projects this may not be considered an issue, but in high risk (sensitive) projects there may be a requirement to authenticate individuals "offline" through direct contact away from the main researchplatform.

With some online forums, individuals may use 'avatars' to create their online identity without providing actual names or images of themselves. In these circumstances the avatar might not appear to be 'personal data' but in many cases the use of these can still be linked back to identifiable individuals. So the same consideration should be given as is the avatar was the individual's personal data.

Recording Consent
Online consent, and the way in which it should be recorded should be proportional to the risk to research to participants. For example, recording consent for 'lower risk' projects might be sufficiently gathered by an individual ticking an online box to say that they accept the terms of participation, whilst 'higher risk' projects which require sensitive personal data may require individuals to complete and return separate consent forms.

In some forums consent may be evidenced via other "implied" means, such as an individual's active participation in a restricted group or through the completion and submission of an online survey, where the survey included a preamble about the purpose of the research and who is conducting it. It may be waived altogether (in the case of data which is truly in the "public domain" *seebelow*).

Where the participants are considered minors requiring parental consent to participate, it may be prudent to garner consent 'offline'.

Withdrawing Consent
As with any research, participants may withdraw their consent at any time during the project. Withdrawal may be as simple as declaring that they no longer wish to participate. Data already gathered at the point of withdrawal will be retained. This is in order to protect the validity of the research and is permissible as an exemption to data subject rights under GDPR.

It is therefore important to know who the chosen system will facilitate such requests – how can you completely delete individual content? How long will content be stored for on the server once it has been "deleted" from the site etc.?

Public Domain or Private
Research that involves mining an existing source such as posts already made on social media or a blogging site should not assume that it's presence on that site means that it is in 'the public domain' and can be used without consent of the contributor. For example, one individual may post on a page or group within Facebook but consider their post "private" because it is only accessible to Facebook members or members of that particular group, whilst another may consider it public because Facebook, or the particular group has so many members. If possible, researchers may wish to direct message individuals to seek their consent to use their post as part of theirresearch.

Copyright
Researchers gathering data, particularly images, from social media must check with the social network provider or site owner to ensure that they have permission to use their content. In most cases, social media networks will claim copyright alongside the original poster meaning that there may be limitations on the permitted use of the material.

For further information about Internet based research the British Psychological Society have produced the useful 'Ethics Guidelines for Internet Mediated Research' which is available here. The Association of Internet Researchers also gives guidance on this topic which is available here.

Guidance for the Use of Mobile Devices for Audio and Visual Recording

Northumbria University takes Information Security very seriously. We invest significant resources to provide students with appropriate systems that they have appropriate tools to conduct their research and to ensure data is protected.

Occasionally however, you may find that you are required to use a personal smart phone or other mobile devices that sit outside of the University and its 'IT Regulations' to undertake audio or visual recordings. As a representative of the University, you are required to ensure that where such devices are used, they are used in an appropriate manner that ensures an equivalent level of security as if they were subject to the University IT regulations.

This guidance covers the use of smart phones and other devices ('device') by students to collect and store information, including audio/visual recordings, for the purpose of conducting research.

Anyone wishing to use a device to gather data may do so, but they must ensure that they do so in line with the following guidance.

Device Security

It is the device owner's responsibility to understand the security features provided by the smart phone/device and to ensure that they are used sufficiently to keep data secure. This includes:

1. Ensuring that the device has installed and configured a tracking and/or remote wiping service (e.g. 'Where's My Droid' for android devices, 'Find My Phone' for windows devices or 'Find My iPhone' for iPhones)

2. Ensuring that the device has up-to-date anti-virus software installed and that it does not block the use of the above.

3. Ensuring that the device 'software updates' service is installed and active to ensure that the latest versions of points 1 & 2 are installed at all times

4. Ensuring that the device includes an automatic locking mechanism which requires a PIN, Password and automatic lock to help protect the device when not in use.

5. Where personal data (as defined by the Data Protection Act 1998) or confidential information is being collected, automatic saving of the device content to personal cloud services is disabled.

6. Automatic syncing with any other personal device is disabled.

7. Information stored on the device is transferred onto your University account at the earliest opportunity and then deleted from the device itself.

8. You do not take a device containing any sensitive information to a anywhere that would be considered a 'high risk' environment (e.g. clubs or pubs where phones are at risk of being lost or stolen)

9. The device is wiped and returned to the 'manufactures settings' prior to disposal – including where it is sold or exchanged.

Loss or theft of your Device

In the unfortunate event that your device is lost or stolen you must:

- Report the loss to the police and obtain a crime reference number.

- Use the remote wiping service to ensure that any data held on there is removed.
- Report the theft to your service provider so that they can also take preventative action against the phone being accessed
- Notify your Faculty immediately, or at the earliest opportunity of the loss (i.e. next working day if lost at night) and assist them with any investigation, should one be necessary.

Monitoring of your Device

The University cannot actively monitor the content of your personal devices, so the onus is on you to ensure the privacy, integrity and confidentiality of any data you store on them.