Section 1: Introduction

Why it matters.

This module is for UCL staff and students who are involved in research with human participants or with information that relates to humans. It covers key points that need to be considered so that everyone across UCL is managing personal data related to research in accordance with:

- Data protection legislation (General Data Protection Regulation 2016 (GDPR)).
- The Data Protection Act 2018 (DPA).
- The common law duty of confidentiality.

These three pieces of law govern how we should manage people’s personal information. They are referred to collectively within this module as data protection legislation.
**Why Data Protection matters.**

Learning about Data Protection will be useful to many people, whether you are supporting the administration of a research project, liaising with researchers and participants or actively part of research data collection and analysis.

If you are involved - in any way - in delivering research, then you need a thorough understanding of data protection legislation. Even if you will later anonymise the personal data you are working with, you are still processing personal data in terms of the legislation as it is personal data up until the point of anonymisation.

And if you are provided with an anonymised data set to work with, then you should still check that personal data is not present. Data protection is an essential aspect of best practice research.

It is key to ensuring personal success and contributing to UCL’s status as a global research leader. Each member of UCL, whether staff or student, has a personal responsibility for handling personal data in accordance with data protection legislation.

This is a legal requirement, but in addition a moral duty. Because we need to ensure that we are trusted by people to process their information with due care and respect. And as a public entity, UCL has an obligation to enshrine best practices into all of its activities. Finally, there can be significant consequences for not complying with data protection legislation, for both the researcher and UCL.
Affected areas.

The consequences of not complying with data protection legislation can impact seven key areas.

• Substantial Damage or Distress to an Individual or Group of Individuals. If personal data is not processed appropriately and is in any way compromised then this may cause real impact to people’s lives. Loss of data or data leakage, as two examples, could be life changing for people - particularly where the data concerned is sensitive and/or the people concerned are vulnerable. The most important reason for complying with data protection is to provide proper safeguards and consideration to all people who are part of UCL’s research endeavours in any way.

• Loss of Your Reputation. Non-compliance can mean reputational damage to both the organisation and you as an individual. If your research is profiled in the national media as having contravened the law, it may have serious repercussions. The national media often run stories on information security breaches which detail how named individuals have lost information and describe the impact disclosures have had on ordinary people. You do not want to be a subject of such attention! Even more critically, you do not want to know you have inadvertently damaged someone’s life.

• Loss of Professional Status. It is not only UCL as an organisation that may be affected. There may be consequences for your career if you have not complied with the law: see UCL’s misconduct procedure for further details.

• Loss of research funding. Research funders will not support research in universities that do not have strong data protection frameworks in place, which includes evidence of completed training.

• Loss of data access. Participants will not want to take part in research at universities perceived not to care about individuals’ information. In addition, key research partners may withdraw UCL’s access to research data if there are data protection failings including lack of proper security processes. There would be an enormous impact across UCL if for example, the Department of Education, NHS or Office for National Statistics withdrew resources from UCL following a serious data protection failing. This would significantly impact many of our research programmes.

• Loss of students. Everything we do has an impact on the profile of UCL. If our research is badly managed, then it will diminish UCL’s reputation more generally and the standing of our global brand, including our teaching programmes.

• Loss of financial resources. Data protection failings can lead to fines of tens of millions of pounds, which would clearly impact on UCL’s overall ability to deliver education and research.
What is personal data?

What is personal data in the context of research?

- Personal data in a research context may be very wide in scope. It is any information relating to an identifiable living individual. It will include direct identifiers such as participants’ names and contact details; detailed research data gathered from participants (for example through electronic tests or paper or online questionnaires); and indirect identifiers such as IP addresses or mobile phone numbers. Personal data will often be embedded within data sets, or files provided by other organisations or researchers. Remember: even the consents you obtain from participants are personal data.

- Sometimes your data may directly relate to a person who is deceased, but this may still be considered personal data if it indirectly refers to other living individuals (for example genetic material and issues related to inherited diseases) which may have implications for a number of people.

- Any act of ‘processing’ of personal data will fall within scope of data protection legislation. Processing is defined very broadly in law. It covers any operation on personal data including holding, storing, creating, sharing or deleting personal data. Indeed, it is hard to find an action on personal data that does not fall within the scope of ‘processing’.

- There are very few researchers to whom this law does not apply. For example, whilst many historians will be using data about people who are deceased, they may undertake activities with participants to transcribe documents or gather perspectives from living individuals, and this will involve processing personal data.

- If you are using personal data gathered by another source, such as a research team in another university, charity or company, you must check that it has been collected and can be used in accordance with data protection legislation. It may be that your own research is not compatible with the agreed purposes for which the data was originally collected. This may mean checking privacy notices and agreements around the use of that data. In addition, the data owner may impose conditions for processing, including how the data can be used and managed; this would normally be detailed in a data sharing agreement or contract.
Special category data.

Some personal data is considered so sensitive that it must be treated separately. One class is called ‘special category data’. Sex life or sexual orientation, racial or ethnic origin, political opinions and religious or philosophical beliefs are examples of special category data (which also covers trade-union membership; physical or mental health; and genetic or biometric data).

In addition to special category data, criminal convictions and offences are another class requiring special treatment. Both of these classes can still be processed for research purposes, but due to their sensitivity, additional protections and requirements are needed.
Designing research projects.

Data protection needs to be considered at every stage of a research project, from initial design through to final publication. This is called privacy by design.

Imagine that you want to undertake a piece of research which involves engaging people as participants or using data gathered indirectly about individuals.

If there is any human dimension to your research, then you will need to think about data protection law from the outset as part of the process of designing the research.

It doesn’t matter if you will anonymise the data later, or if you believe you are using an anonymised set of data you must still take account of the law in your research design, and introduce checks at certain points.

The majority of research at UCL involves people in some way, and so understanding the law is critical. The law does not stop you undertaking challenging research, but you must carefully think-through every stage of the research and data lifecycle.
The research and data lifecycle.

When you are initially planning your research you will think about aims, questions, and any exploration or testing that will be done.

You will develop a research methodology/approach and in deciding this it is important to think about who and what data will be involved.

Will there be interviews, focus groups, medical tests, online surveys, pre-collected data or surveillance? How will you ensure the data gathered is accurate? Will the data be potentially sensitive in any way (e.g. health and wellbeing, or political views)? Are you working with people who are vulnerable, like children? This will influence how you consider the design of your research, collect data, share, protect and manage it through time.

How you collect your data will influence data protection considerations. For example, are you analysing social media? What are the expectations for using output for a particular social media platform? Is the information published or private? Where is the service and where are the participants? What are the expectations for gaining consent or informing people about your research?
Anonymisation.

Often researchers presume that the answer to dealing with all data protection concerns is to anonymise.

- Anonymisation means you must remove any information that can link the information back to an identifiable person and consider whether others hold information that can link the data you hold to an individual.

- Anonymisation is a useful tool, but it is very hard to achieve. For example, it is very hard to claim that data collected from a focus group will be anonymised as all those who participate are likely to be able to track some information to particular individuals within the group. Any narrative data is hard to anonymise.

- In dealing with participants’ personal data it is important to be honest about what the expectations for participation/testing are and what will be public or anonymous. There are circumstances where it is important not to anonymise personal data. You may consider pseudonymisation or identification. You must think about how to manage people’s privacy in the design of the research. This means putting in place appropriate safeguards for the research data and any associated administrative processes.

Here are two examples of safeguards:

- When you email people as a group, use Bcc to hide the recipients, or set up a dedicated mailing list that masks individual email addresses – unless you have the permission of individuals to share their names (e.g. for collaboration purposes).

- When you store the data, you may need safeguards to protect it, such as encryption or access control.

- When you use third-party data, even if it has been anonymised, you must confirm that it was lawfully collected and check if there were any conditions or expectations around further use. If data is from a trusted provider, such as the NHS or UK Data Archive, then this should be clearly set out in their data sharing agreements or contracts. Sometimes you may need to ask research partners for evidence that the necessary consent forms and privacy notices have been put in place.

- If you share the data, you may need to do so under agreed terms. If there is a contract in place with any organisation, there may be specific provisions in place that limit how you can share the data. You will need to think about who you are sharing the data with, why, what you expect that person/team to do with the data and where in the world they are working. There are different data protection laws in other parts of the world, but wherever you transfer the data it must meet the standards and protections set out in data protection legislation. You will need to check the current guidance on UCL’s websites when any information is transferred overseas.
Anonymisation and Pseudonymisation – Additional details.

There are a number of myths about data protection and one is that all data should be anonymised as soon as possible. This is not true. There are justifications for retaining data which does connect it to living individuals. For example, research data where the participant requires credit and acknowledgement for all contributions to be made public. Another example is a longitudinal study where you need to track responses linked to an individual over time. However, anonymisation is a powerful tool for most researchers. Anonymisation can assist with data management by protecting people and their research participation. It aligns to principles of good research ethics and practice on occasions when it is judged appropriate to anonymise. In addition, once properly done it means that data protection legislation no longer applies.

Anonymisation means stripping out any personal identifiers to the extent that it is impossible to re-identify anyone from the data. Anonymised data cannot then be linked to an individual. You should consider taking steps to anonymise personal data as it can protect individuals’ privacy.

If you do decide to take steps to anonymise the data, it will still be personal data up until the point the data is anonymised and must be managed carefully in line with data protection legislation. Indeed the act of anonymizing is an act of processing. You should take note that it is getting harder and harder for researchers to achieve full anonymisation because, in some cases, information from other publicly available sources, such as social media, could be combined with the anonymised data to re-identify individuals. In addition, digital forensic experts can sometimes reveal hidden identifying information, for example a word document will have hidden data in the word file. Some data cannot be anonymised, for example samples relating to rare diseases. Even if a name is removed it may be possible to connect data with an identifiable person. It is argued that datasets with three or more indirect identifiers may not be classified as anonymised depending on the identifiers.

An alternative step to anonymization is to use pseudonymised personal data. This is where the data can no longer be attributed to a specific person without the use of ‘additional information’. This ‘additional information’ allows you to re-identify individuals. You must keep this ‘additional information’ (such as a key-code) separately and protect it with appropriate safeguards, e.g. encryption or access controls. Pseudonymised personal data is classed as ‘personal data’ and so data protection legislation still applies.

One of the main benefits to using pseudonymised personal data is to limit the risk of accidental or unintentional disclosure by minimising how many people have access to identifiable information; this significantly reduces the risk of a data breach.

Remember if you get pseudonymised personal data from another organization or partner this is personal data in their hands as they have the key, i.e. the ‘additional information,’ to be able to re-identify individuals. In your hands it is likely to be anonymous data because you do not have the key to re-identify individuals.
Anonymisation is a science in itself so in practice determining the extent and robustness of anonymisation / pseudonymisation can often be difficult. Ultimately, decisions should be made by the Principal Investigator/Supervisors for students' research with support from the ICO's Anonymisation Code and advice from UCL’s Data Protection Office. It is important to document how these decisions have been made. This will enable future accountability and a check on the robustness of the processes.
Outputs.

From the outset, you should think about what you want to achieve in terms of potential outputs, publishing and promoting the research.

Do you need to quote individuals? Will you deposit the data set in order that others can use it? Do you need to gather impact data from people about how they have benefitted from the research? Each of these activities means you will be managing personal data.

In most cases it will be possible to carry out such activities and achieve your research aims, but you will need careful research data management at each stage of the research process to ensure that you do so in accordance with the law.
Documenting decisions.

It is important to document your decisions for three reasons: it will help you to plan your research properly including how you will collect data, what data you will collect and what you do and do not need in terms of consents and agreements; secondly, to comply with the principle of accountability in data protection legislation; and thirdly, this log will be your defence should something go wrong.

For this reason, researchers are encouraged to put data management plans in place.
Another tool which helps you manage your data is a Data Protection Impact Assessment, sometimes called a Privacy Impact Assessment. This can be a very helpful aid to managing information in complex contexts. For example, if you need to travel with your research personal data on a laptop, it’s good practice to undertake a Data Protection Impact Assessment first, to show you’ve considered the privacy risks.

The Assessment documents key decisions and how you arrived at them; what minimum data is required for your research purposes; why it is needed; and how it is protected (e.g. the laptop could be encrypted).

Were your laptop to be lost or stolen, the Assessment would demonstrate you had considered the data protection implications. This would be part of a defence should there be any investigations by UCL or the Data Protection Regulator – the Information Commissioner’s Office.
Section 2: Data Protection Responsibilities.

A shared responsibility.

Every member of UCL, whether staff or student, has a specific responsibility for handling personal data in accordance with data protection legislation.

For staff research, Principal Investigators will be accountable for ensuring that their projects are managed to comply with all data protection legislation.

For student research, Principal Supervisors are responsible for ensuring that students under their supervision follow data protection requirements when processing personal data as part of their UCL programme of studies.

This means that the Principal Supervisor will guide the student on their planning and processes.

However, the student is then responsible for ensuring that they follow this guidance in practice.

All research projects where personal data is processed must be managed in accordance with the requirements of the UCL Data Protection Office.

This means managing personal data at every stage of its collection or creation, including just storing it and when it is shared or published, in compliance with data protection legislation.

In the context of UK data protection legislation, the regulator for data protection is the Information Commissioner and the Information Commissioner’s Office – or ‘ICO’ – enforces data protection law throughout the United Kingdom.

If you are undertaking research in conjunction with another organisation, then you will need to agree the different data responsibilities.

And if anyone is processing data on your behalf, for example a transcription service, then you must have a data processing agreement.
Controllers and Processors –
Additional details.

The organization that determines the purpose for processing the data in a research project is the Controller. Controllers can be individuals but more commonly they are organisations, such as UCL. For research undertaken at UCL, UCL is almost always the controller with the main responsibility for the burden of compliance. However whilst UCL does have this overarching responsibility for compliance, all individuals who do not take steps to work within the law may face personal consequences. This training forms part of a set of UCL resources to support individuals in understanding their responsibilities.

When research is done collaboratively with other researchers at organisations outside UCL the relationships and responsibilities between the organisations need to be understood. It is possible to have Joint Controllers, for example where UCL is engaged in collaborative research with another university and both organisations are working jointly on the project with joint responsibilities for the personal data. These roles, and their respective responsibilities, need to be agreed at the outset and best practice dictates that this should be a documented position within a data sharing agreement. You can download a template Data Sharing Agreement form from the UCL data protection site or use one provided by the other Joint Controller provided it covers all the same points. If for any reason you do need to use a more bespoke agreement then you must check this with the Research Contracts team for advice.

A Processor uses personal data on behalf of the Controller. If an external processor is used, a data processing agreement must be agreed and signed by both parties which provides clear instructions on how personal data should be used. This is mandatory under the law. It is the responsibility of the principal investigator / research lead to ensure this agreement is put in place. Students must flag to their Principal Supervisor the personal data processing work flows for their research, i.e. how, where and by whom data is processed. Principal Supervisors will then work with students on any required documentation. You can download a template Data Processing Agreement from the UCL Data Protection website. Sometimes data processing agreements will cover a commercial relationship, for example a company offering a transcription service for audio recordings. It is not appropriate to make informal arrangements for example with family and friends. You must put in place a processing agreement when you use a commercial service and some processors will provide such an agreement.

This must be reviewed to ensure it does cover all your expectations in terms of what will be done with the data. It is important to ensure that the processor understands and can comply with the confidentiality involved in this work, keeps the information securely and in server spaces that comply with the law, reports any breaches to you within 72 hours, and returns or purges any content from their systems at the end of the work. You may need to work through this with the processor to ensure that they understand what is required. Supervisors will need to support students on these processes.

Research Contracts can advise on data sharing and processing agreements for research projects.
Registering your research.

Please note: This research training and the completion of the module assessment is mandatory for all staff and students with any involvement in research.

All staff and Doctoral students are required to register their research with the Data Protection Office.

Undergraduate and Postgraduate students (excluding Doctoral Students) may be exempt from the requirement to register, provided that they meet the requirements covered on this screen.

Exemptions exist where students have successfully completed this research information compliance training and the final assessment. They must also have had their project signed off by their Department, with no further action having been deemed to be required.

On some occasions the Department will require that the research is registered, and further data protection advice sought. For example, this may be necessary when the research involves special category data, vulnerable people or surveillance.

It is important for all staff and students to understand the specific local guidance and support networks within their own Departments.
Special category data.

Please note: You may require more specific advice if you are handling special category data, such as health data, or extremely sensitive data, such as criminal records data.
Section 3: Lawfulness, consent, fairness, transparency.

Lawful processing.

At the heart of the rationale for managing personal data is a desire to deliver research which will benefit society. Data protection legislation requires UCL to ensure that all personal data is used lawfully. To lawfully process personal data one of six lawful bases need to be met:

- Vital interests.
- Legal obligation.
- Contract.
- Public task.
- Legitimate interests.
- Consent.
Basis for processing.

The legal basis for almost all of UCL’s processing of personal data for research purposes is ‘public task’.

This is because, as a university founded under Royal Charter, UCL is a public body with research as a core purpose of its public delivery.

Thus, for UCL, personal data processed for research is lawful as a ‘public task’.

There may occasionally be other lawful bases for undertaking research, such as studies undertaken as part of a legal obligation, or for the vital interests of someone, but these will be very rare.

An example might be where the research is life-changing for the individuals, but the circumstances do not enable consent, for example in some complex warfare or refugee situations.

And when special category personal data and data relating to criminal convictions and offences is processed, there must be a further legal basis for the processing.
Legal bases: FAQs

What is the legal basis for processing special category data?

- For almost all instances of research conducted at UCL the legal basis for processing special category data will be research in the public interest purposes, i.e. that the processing is necessary for archiving, scientific research, historical research or statistical purposes.

- There are other legal bases, such as explicit consent, vital interests, legal or court claims, but you should not rely on these without guidance from the Data Protection Office.

Is market research a lawful basis for processing data?

- The lawful bases for research do not include ‘market research’, which isn’t deemed to be in the public interest in the same way. But you can use market research data and obtain participants through market research companies. If a company initially gathered the data for its own purposes (i.e. was the data controller) you would need to ensure it had permissions enabling it to pass on this data.

- Participants would be expected to have ‘explicitly consented’ that the company could collect and share their data for third-party research: so explicit consent would be the lawful basis for processing. If the company was acting as a processor under instructions from UCL, then this would be a public task and the company would be acting under contract. You’d need to ensure the company delivered and gathered the market research in compliance with the law, via a Data Processing Agreement.

Is ‘consent’ a legal basis in all countries?

- No. You should remember that other countries have different legal bases for consent.

-
Consent.

For research purposes, there are two different types of consent.

- GDPR consent governed by data protection legislation (a legal basis): Under data protection legislation, although GDPR consent is one of the lawful bases for processing, staff and students should not normally rely on it for processing personal data for research purposes. Instead, you should normally rely on ‘public task’ as the lawful basis.

- Informed ethical consent governed by common law: Even though you should usually rely on ‘public task’ as a lawful basis, informed ethical consent is still important. In order to comply with accepted ethical standards for research and to obtain ethical approval for a project, researchers will generally need to obtain the informed ethical consent of individual participants for their involvement in the research. This is supported in data protection legislation because researchers must act in a manner that is ‘in keeping with recognized ethical standards for scientific research’ - and fair. As such, research regulators will usually expect informed consent.
Research Ethics Committee.

To be sure you are following the right guidance, UCL’s Research Ethics Committee provides a list of the appropriate ethics committees for your research and you should follow their guidance about consent.

If, for example, your research involves NHS patients and/or their data, you should refer to the Health Research Authority’s Guidance. Where you need to apply to UCL’s Research Ethics Committee, it too will usually expect informed ethical consent.

This will include explaining to participants whether or not they can ask for their data to be erased, and potentially, at what point this is no longer possible, for example once their data has been aggregated with others or it has been rendered anonymous.

You should note that where it is impractical to seek consent for use of NHS data, Section 251 of the NHS Act 2006 provides an exemption from obtaining direct consent. Note also that there are variations between England and Wales, Scotland and Northern Ireland.
A legal requirement.

Under data protection legislation, there is a requirement to use personal data fairly and transparently. In practice, this means telling people about what you are doing by providing a privacy notice that explains how participants’ personal data will be used, the purposes for which it will be processed and how it will be handled. There are strict requirements about what information should go into a privacy notice.
Privacy notices.

UCL has developed two compliant privacy notices for research purposes that staff and students should normally rely on to meet the requirements of a privacy notice, one for general research and a specialised notice for health or social care research. The latter may provide additional points for consideration in other research projects where there is special category data, for example psychology studies.

Researchers should put a link to the applicable privacy notice within participant information sheets to ensure they meet the fairness and transparency principle in data protection legislation. This has been incorporated into the overarching Research Ethics information sheet and consent templates. However, you must check that the privacy notice linked to does cover how you are processing personal data for your particular research.

Where further information is required (to be fair and transparent) or you have particular project-specific information that may affect participants’ privacy, you should provide it as part of your participant information sheets or local privacy notice. In this way, your participant information sheets will supplement the general privacy notice for research purposes. For example, in your study it may be possible to remove data relating to individuals at an early stage in your research, but not once it has been amalgamated for analysis. You should explain to participants that at this stage it won’t be possible for them to have their data removed.

If you do develop your own privacy notice as part of your participant information sheet, it’s strongly recommended that you still link to one of the UCL templates provided with the data protection materials on the module website.
Special circumstances.

If you are undertaking surveillance research (e.g. filming or monitoring exchanges without individuals’ knowledge) then you can’t necessarily provide a privacy notice in the same way.

This doesn’t mean this kind of research can’t happen, but you need to further document and consider the legal bases for processing, and the framework of safeguards needed. You would need to undertake a Data Protection Impact Assessment. There are some circumstances where you should consider if you can collect personal data in the way you have done previously. In such instances the Data Protection Impact Assessment will help you think-through your data research processes.
Section 4: Documentation, impact assessments and safeguards.

Introduction.

When designing a research project, data protection requirements must be considered from the outset in order to embed proper controls and processes at each phase of the research.

This is termed ‘privacy by design.’ It helps all those involved in the current research and potentially also in future research to manage and maximise the use of the data through time.

This includes assigning data protection responsibilities and considering all aspects of the data processing. Best practice dictates that you should have a Research Data Management Plan and some research funders will dictate that this is a requirement.

A Research Data Management Plan will record all of the personal data which will be collected or created as part of the research.

It will determine the conditions for processing that data and set out how the data will be shared where it will be held how it will be protected, and if it will be formally archived or destroyed.
Ethical considerations.

Some things you will consider within your planning may relate to good ethical research practice, rather than data protection legislation specifically. Separately, you must also consider and fulfil the Research Ethics requirements which are not covered in detail within this module.

At all times, you must comply with UCL’s code of conduct for research and any other relevant professional codes of conduct.

Research ethics, like data protection, ensure that your research is properly managed, fair and credible. It takes into account new and evolving societal expectations. So ethics protects your participants, your research reputation - and UCL as a whole.
Appropriate Safeguards – Additional details.

Researchers must manage personal data using the following appropriate safeguards:

- Collect only the minimum amount of personal data required to carry out the research.

- Make sure the personal data collected and managed is accurate and reliable. Not only will this help you comply with data protection law but it is a key part of good research. You do not want to be analysing unreliable information.

- Use pseudonymised personal data (or even better, anonymised data) where appropriate and possible. There may be occasions when you need to retain the identifiable personal data but make sure you then consider putting in place protections such as those listed below.

- Implement safeguards against accidental disclosure and loss or corruption of research data, including:
  - Technical controls such as encryption on laptops, USB sticks and files. (Encryption uses an algorithm to transform information to make it unreadable for unauthorized users. It is different to and a far stronger protection than a password.)
  - Safe data storage such as use of the UCL Data Safe Haven. This is a special storage area that stops information being accessed or distributed without permissions. The project owner will manage these permissions. It also ensures data deletion.
  - Regular backups, to guard against loss of data (these need to be kept as securely as the original copy of the data)
  - Physical security such as locks and privacy screens on laptops
  - Research data management plans to think through adequate safeguards.

- Protect the personal data to ensure that it is not compromised and thus you avoid causing substantial damage or distress to any individuals.

- Ensure that the processing will not be used to support measures or decisions with respect to a particular individual.

- Comply with relevant ethical standards and seek ethical approval for your project

When you are managing personal data think about how to maintain its:

- Confidentiality – this means protecting information where there is a need to maintain the confidentiality. On some occasions, participants will specifically require credit for all their contributions.
- Integrity - this includes taking steps to ensure that the data collected is accurate, reliable, and protected from accidental or malicious modification
- Availability – data will need active management through time to ensure it is available when needed.
CIA is a helpful acronym to remind you of these three areas of consideration.

These appropriate safeguards are crucial for researchers because unless they are in place it will not be lawful to use personal data for research purposes.

How the safeguards should be used will depend on the type of personal data that needs to be protected. For example, some data such as contact details can be saved on mobile devices provided they are properly encrypted and there is a further protection, such as a strong password or PIN code to unlock.

You should consider whether data is taken offsite. All staff and students have allocated storage space on the UCL servers. This means data can be accessed from home through Desktop@UCL Anywhere. Some personal data should not leave the UCL Data Safe Haven. This is determined by considering the data and the implications and risks if the data were ‘breached’. A Data Protection Impact Assessment will help when considering what blend of appropriate safeguards are needed for managing personal data.

It is also important to review who has access to the data, so that anyone leaving the research team can no longer have access. Similarly, any systems that hold sensitive data should only be re-used for other purposes once the data has been securely deleted.

In addition, the Research Integrity Training Framework will help put in place strong research structures.

Further information on safeguards is available on the UCL website.
Avoiding damage.

When thinking about the management of personal data, you are trying to avoid causing an individual or any group damage or distress. This can be in material form, such as financial damage or identity theft, or non-material form, such as reputational damage or embarrassment.

Other types of damage or distress might include examples of processing that give rise to discrimination, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage. Accidental use of ‘Cc’ instead of ‘Bcc’ in mass email is a common cause of data breaches where damage or distress can arise.

There are some types of research which due to the public benefits derived from the research will be considered acceptable even if an individual is ultimately caused damage or distress. For example, when a patient is prescribed a placebo drug in a controlled trial and monitored. Whilst this may ultimately damage and distress a patient, the public interest in this approach is accepted.

Another example is research into criminal activities. The rights of the criminal to privacy when criminal activities are occurring clearly differ than those of other citizen actions. Nevertheless, you may still have some confidentiality and privacy obligations. You should seek ethical advice before embarking on such research.
Additional consideration.

Children, criminals, patients and people without capacity.

To ensure that your study is fair and transparent for data protection purposes, some individuals or groups will require additional consideration in terms of whether or how they can consent and if they require additional protections.

Particular groups include children, criminals, patients/clients in terms of medical and other types of health or social care interventions, and people without capacity to make decisions. For example, in England and Wales this is set out under the Mental Capacity Act 2005. Legal definitions of capacity will differ around the globe.

In addition to Data Protection Registration processes, the Research Ethics Committee will normally review research concerning vulnerable individuals. The NHS Research Ethics Committee will also look at relevant applications.
International issues.

What if personal data is transferred outside the EEA?

If research involves transfers of personal data outside the EEA, appropriate safeguards should be put in place as the data protection legislation and level of protection will differ from that within the EEA. There are different requirements in terms of safeguards, depending upon the countries involved and the personal data. Transfers of personal data can occur if you or a Processor you are using are based overseas, or if you are working with a researcher from another non-EU university. You must check which countries the data will be processed in (such as via an online survey tool or email/data sharing service). UCL has published a Guidance Note on this subject and continues to provide up-to-date advice on transfers of personal data outside the EEA.

What safeguards are required?

A Data Protection Impact Assessment is recommended to help you evaluate where and how to store information and how to put in place appropriate safeguards. A Data Protection Impact Assessment should always be undertaken for higher risk research. You can check this on UCL’s Data Protection Impact Assessment’s guidance page.

What do I need to know about laws in other countries?

Different relationships and requirements are in place for working with different countries. Further information is kept up-to-date on these relationships on UCL’s main Data Protection site. You may need to take into account the specific legislation for the country you are working in. There may be different legal bases for processing personal data and gaining consents.
Security breaches.

If you were to have a security incident or even a near-miss, then you must report this quickly using the Personal Data Breach Reporting Form. UCL must take urgent action to minimise the impact. Such incidents must be reported to the regulator within 72 hours. This includes non-working days (i.e. Saturdays and Sundays) and public holidays, so you need to act promptly.

Email the completed form to the UCL Information Security Group. You must not report the incident directly to the regulator (the Information Commissioner’s Office - ICO) or media. This is something that UCL’s professional experts will judge and then, if needed, ensure that the right information is provided.
Reporting incidents.

Security incidents can be very wide-ranging, from being hacked, sending an email to the wrong person, making an unfair disclosure by using CC instead of BCC, losing information or a device, or data being corrupted.

If you are in doubt about whether to report an incident, err on the side of reporting. UCL can judge what the best steps are, and help you manage the incident. Failure to report incidents can lead to serious problems - so ensure you act, and act promptly.
Retention and future use.

When considering how long to keep the personal data you have collected, ensure you observe UCL’s records management procedures and records retention schedule.

When you deposit data in an archive or with a Journal article, make sure you include all of the necessary documentation. Do not deposit identifiable data unless you have specific consent to do this. Any data deposited must have the correct data protection approvals and ethical consents. If you get this right, then your research data is more likely to be able to be reused, and benefit research endeavours over future generations.

Always follow the guidance produced on Open Access.
Section 5: Individual rights.

Overview.

Individuals are given specific and formal rights in data protection legislation. These are covered in UCL's introductory GDPR training module. In essence, individuals in most research contexts have the right to be informed about the research, and how data is handled. Individuals may also make requests under the law, including requests for copies of their information, for data to be amended and for data to be erased. Requests relating to these rights must normally be answered within a month.

However, many of these individual rights are exempt for research purposes. There will be specific considerations for certain types of data, such as NHS Digital. For all formal Data Protection requests you will need guidance. In addition, the request needs to be answered in a very specific legal way. If you receive any such request, you must forward it to the Data Protection Office, marking it as urgent.
Module conclusion.

Data protection within research is an extension of good research practice which the public rightfully expect. You will be considering many aspects of data protection when you complete your research ethics application form and participant information details.

Good use of personal data within research involves thinking of the way you will use the data in detail at the start of your project. Pre-planning in this detailed way will benefit the research by ensuring that data is managed appropriately, and that you can use it as you require, potentially also sharing the data at a later stage. Rigorous planning of research is a central aspect of good research practice!

Further guidance is provided on the module website, including a MythBusters guide!
Credits.

Project Lead:
Kedisha Taitt.

Author:
Dr Elizabeth Lomas.

Editorial Team
Kedisha Taitt,
Dr Elizabeth Lomas,
Lee Shailer,
Trevor Peacock,
Dr Nathan Lea,
and
Alex Potts.