# C:\Users\james.austin\Desktop\OU_Logo_Dark_Blue.jpg

# **Research Degrees**

# **Research Guidance**

A. Data protection principles

B. Specific processing situations

C. Individuals’ rights

D. Exemptions

E. Checklist

1) Start the HREC and/ or SRPP processes, as required

2) look at the Data Protection screening questions – is your activity high risk? If so, you’ll need to complete a DPIA and submit this to data-protection@open.ac.uk

3) Register your data on the Information Asset Register – this will enable you to get a number for SRPP. Please do this via your I[nformation Governance Liaison Officer](https://openuniv.sharepoint.com/%3Aw%3A/r/sites/info-compliance/dp-compliance/Policies%20forms%20and%20templates/Information%20Governance%20Liaison%20Officers.docx?d=wd82a879b93f847c0be5fea0c5de89dfe&csf=1&e=Mjg1Ie) or directly to data-protection@open.ac.uk

See <http://intranet6.open.ac.uk/governance/data-protection/ou-data-protection-procedures>

4) Check the data protection guidance below:

## **Data Protection Principles**

### **Informing participants: your Participant Information Sheet**

You will need to include “privacy notice” information in your Participant Information Sheet (See Number 14 on the following link). See <http://www.open.ac.uk/research/governance/ethics> for examples, and guidance from the [Information Commissioner's Office.](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/)

If you are conducting scholarship and using existing student data, this is covered in the [Student Privacy Notice](https://help.open.ac.uk/documents/policies/privacy-notice), and generally you will not need to notify students about what you are doing. Bear in mind that quotes from assessments should not be published without notification/ consent: see [Assessment Handbook](https://help.open.ac.uk/documents/policies/assessment-handbook) section **2.3.3 Confidentiality of assignments and other assessments** *All information you give in assignments and other assessments is regarded as confidential to you, your tutor or practice assessor, the marker, and the University, and won’t be divulged to anyone outside the University. However, some programmes have additional confidentiality guidelines and data protection rules which you will be told about in the assignment guide for your module or your programme-specific information.*

* If your research subjects are students or members of staff, you can link to the relevant privacy notice to cover aspects like the data controller, Data Protection Officer contact details, and the data subjects’ rights
* If the OU is the data controller (rather than e.g a lead partner organisation), you could link to <http://www.open.ac.uk/about/main/strategy-and-policies/policies-and-statements/website-privacy-ou> if you want to use this to cover Data Protection Officer contact details, and the data subjects’ rights etc.
* You should give people the opportunity to agree to participate only in certain areas of research or parts of research projects (Recital 30).
* You will need to identify the “lawful basis” for processing personal data to put in the participant information sheet/ privacy notice. If you are conducting academic research for potential publication, your legal basis is likely to be that it’s necessary for our **public task** of conducting academic research. If you are conducting research primarily to improve the OU’s services, then your legal basis is likely to be that it’s in our **legitimate interest** of improving our services.
* You should consider whether you can fulfil all data subject rights, or whether doing this will impede the purpose of the research – see “Data Subject Rights.”

#### **Consent**

For all research where personal data is collected or used, regardless of the data protection legal basis used, we will ask for ethical informed consent from participants. It is helpful to distinguish this from consent as the legal basis for processing personal data:

* + If you use consent as the legal basis for processing the personal data, then you need be able to deal with consent withdrawal at any time up to the destruction or anonymization of the personal data – even after publication or aggregation of data.
	+ If you can do this, you may want to consider using consent as it could mitigate some risks to the data subject, e.g. if they are particularly vulnerable or the research is particularly intrusive

When gaining ethical informed consent, generally you would offer the opportunity to withdraw from research and have participant data erased up to the point that data is aggregated or published. This corresponds to the “right to object” under the **public task** legal basis.

## **Storing consent forms**

Signed consent forms should be stored securely, either as physical or digital copies. Physical copies should be in a locked drawer/cabinet, within a locked office. Digital copies should be encrypted and located separately from the research data. This could be in a separate storage system or volume (e.g. with administrative data) or in the same system or volume but within a separate, access controlled ‘folder’ with access limited to those who need it. For example, in a SharePoint collaboration site, in a distinct folder, accessible only by the PI.

Signed consent forms should be kept for as long as personal data is kept. Once data is no longer identifiable, it is no longer considered to be personal data, so at this point signed consent forms should be destroyed.

A blank (unsigned) template of the consent form and information sheet should be kept and archived with the research data, to record what participants were told and asked to consent to.

## **Processing “special category” personal data**

If you are processing “special category personal data” you need to

* Document your condition for processing in the Information Asset Register- This is likely to be that is necessary for scientific/ historical research and in the public interest.
* Ensure that the research is in the public interest.

Special category data includes information about

|  |  |
| --- | --- |
| * Race
 | * trade union membership
 |
| * ethnic origin
 | * health data
 |
| * political opinions
 | * sex life or sexual orientation
 |
| * religious or philosophical beliefs
 | * genetic data and biometric data (where this is used for identification purposes)
 |

Information relating to criminal convictions and offences also requires a higher level of protection

### **Using data for other purposes**

Generally, you must only use personal data for the activities specified in the privacy notice when the data was collected. However, you may undertake research using personal data which has already been gathered for a different purpose. (Recital 50 states that research is always a “compatible purpose”)

If you are going to use data which has been gathered for a different purpose, you should still inform the data subjects about what you are doing with their personal data. The only exceptions to this are

* Where the data subject already possess this information
* Where this proves to be impossible or would involve a disproportionate effort. The number of data subjects, the age or the data and any appropriate safeguards adopted should be taken into consideration when identifying if the effort is disproportionate. If you take this approach, you should document your decision and rationale.
* You are likely to need ethical consent to use the data for this further purpose

If you don’t know all the purposes which data will be put to when you gather it, you should suggest potential types of use in your privacy notice.

NB when re-using existing data, all the data protection principles and guidance in this document still apply.

### **Anonymisation and destruction**

You will need to plan to delete any personal data which is no longer required. If the personal data will be required, then you may retain it, but you need to have articulated a reason for this.

You must anonymise as much data as possible – so that it can **never** be linked back to the individual (“re-identified”).

NB if you still retain the original data, it is likely that you will be able to link the data back to the individual. At this point it is no longer considered personal data. If you completely anonymise personal data, you should destroy signed consent forms at this point.

If you cannot anonymise data, then you should pseudonymise it as far as possible: this means to remove the name and any other direct identification but retain a link to data which identifies the individuals – this is a security measure.

If a means to re-identify exists, for example a key record of participant names which have been replaced by codes or pseudonyms in the dataset (even if this is kept separately and securely) the data cannot be considered anonymised. It is instead pseudonymised, is still subject to data protection legislation, and signed consent forms should be retained.

It is possible that guaranteeing true anonymization of data cannot be guaranteed, as combining with other datasets and the development of technologies in the future could potentially re-identify people. Also, in cases where focus group data is collected it is often difficult to assure full anonymity because the researcher cannot make the other participants keep the information, they hear from others confidential. However, to retain signed consent forms or other records of participants on this basis itself creates a risk of identification.

So if data has a been fully anonymised to the best efforts and judgement of the researcher, where it is not possible to predict future technologies or techniques that could combine anonymised datasets to re-identify participants, data should be considered ‘anonymised’ and signed consent forms should be destroyed.

[EU Data Protection Working party guidance on anonymisation techniques](http://www.dataprotection.ro/servlet/ViewDocument?id=1085)

[Irish information commissioner advice on anonymisation and pseudonymisation](https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm)

You may store, or archive, personal data for future analysis if all other safeguards as described in this guidance are taken.

Good [information management](http://www.open.ac.uk/library-research-support/research-data-management) and email practices help with this.

### **Integrity and confidentiality (Security)**

* Only those who need to use personal data should have access to it
* You must have organisational and technical measures in place to protect personal data from unauthorised access, use and destruction, whether malicious or accidental.
	+ Usb sticks and other portable devices must be encrypted
	+ Use locked bags when moving papers
	+ Use OU devices and OU systems wherever possible, rather than personal devices and accounts
* You should ensure that data is held on OU (or partner agreed) systems with appropriate access controls; that paper is kept locked away, etc
* See the [Information handling guidance](https://openuniv.sharepoint.com/sites/intranet-it/Shared%20Documents/The%20OU%20Information%20Security%20Policy%20Set%20for%20All%20Staff%20and%20Contracted%203rd%20Parties%20V1.6.pdf) and [information security policies](https://openuniv.sharepoint.com/sites/intranet-it/Pages/information-security-policies.aspx)

### **Data minimisation and accuracy**

* You must only collect personal data that you need to carry out these activities – It must be adequate, relevant and limited to what is necessary.
* You should ensure that wherever possible, data is pseudonymised (recital 156). This means that you can keep details of the participants, but keep their real personal details separately from the data, and use IDs or nicknames to identify the records. See section 5 below for more information.
* Make sure that the data you collect and use is accurate
* If necessary, you must keep personal data up to date so it is fit for purpose. This is more likely to apply to mailing lists etc, rather than personal data gathered for analysis

## **Specific processing situations**

### **Contracts**

If you are conducting research with partners and transferring personal data to or receiving personal data from other organisations, then you are likely to need some kind of contract or data sharing agreement.

* Identify the data controller(s): this is the organisation(s) specifying the purposes for processing the personal data, what personal data is necessary, how it will be maintained and secured, and how long it should be kept for.
* If any organisations share a purpose for processing the personal data, then they will be joint data controllers, and a data sharing agreement is required. If there is a formal contract between the parties, this can be set out in a contract addendum. If there is not a formal contract, then you will need a separate data sharing agreement setting out the responsibilities that each organisation has for processing the personal data.
* If the purpose for processing the personal data is different for each data controller, then a data sharing agreement is advised, but not absolutely necessary.
* If the OU does not specify the purpose for processing the personal data, but instead carries out the instructions of another organisation, then it is a data processor. There must be a contract in place setting out the terms of the data processing.

### **International transfers**

If any data is transferred, processed, stored or viewed outside the EEA, then additional safeguards need to be put in place. The most likely circumstance is that “model contract clauses” are required in the contract between the organisations.

This includes if personal data is handled by overseas contractors or stored with cloud computing services with servers outside the EEA.

Alternatively, you could share data overseas if you have **fully anonymised** it, i.e. destroyed the raw data you collected, so the personal data can never be reidentified.

If you only receive data from overseas, but do not transfer it back overseas, then you don’t need these additional safeguards.

If you work with overseas partners who use contractors to handle data processing, then the contractors and contracts only need to be compliant if data is transferred to them from the UK/ EU.

### **Children**

If you are conducting research on children, you will need to follow HREC guidance on consent and parental consent. Any documents directed at children must be intelligible to them.

If you are providing online-only services directly to children under 13, and your legal basis for using their personal data is consent, you must

* Have some kind of proportionate mechanism for confirming that the data subject is over or under 13
* Gain parental consent for data subjects under 13
* Check that the consent has been given by an adult with parental responsibility – proportionately depending on the risk to the child of using the service

### **C. Individual Rights**

You must be able to fulfil data subject rights, where they are applicable.

The following rights apply where the lawful basis for processing is that it is part of our public task (which is likely to be the case for most research.) However, we can consider not fulfilling these requests if they would prevent or seriously impair the research purposes (DPA2018 Schedule 2 part 5 based on GDPR art 89)

If you want to use these exemptions, you must ensure that processing personal data for scientific or historical research purposes[[1]](#footnote-2)

* + will not cause damage or distress
	+ must not make decisions about individuals unless for the purposes of approved medical research
	+ is necessary for the research (GDPR Article 89 and DPA 2018 section 19)

|  |  |
| --- | --- |
| **The right of access**  | Can you provide all the personal data you have to the individual if requested? (NB fully anonymised data no longer counts as personal data) |
| **The right to rectification**  | Can you rectify inaccurate personal data, or complete it if it is incomplete?  |
| **The right to restrict processing**  | Can you restrict data if necessary? E.g. by temporarily moving the data to another processing system; making the data unavailable to users; or temporarily removing published data from a website.  |
| **The right to object**  |  If the lawful basis is legitimate interest/ public task, you must consider whether you have compelling grounds to override the request of a data subject, in their specific situation, to stop processing their data. This equates to the ability to withdraw from research up to a certain point. |

The following rights apply where the lawful basis for processing is consent. If you have identified that consent is your lawful basis, rather than “public task”, then you will need to be able to fulfil these reuqests

|  |  |
| --- | --- |
| **The right to erasure** | Can you erase data on an ad hoc basis?NB this is not applicable if the lawful basis for the research is that it's part of our public task, and we still need the data.  |
| **The right to data portability**  | The right to data portability only applies when your lawful basis for processing this information is consent **or** for the performance of a contract; and you are carrying out the processing electronically  Can you provide the personal data on request in a format that is: * structured;
* commonly used; and
* machine-readable.
 |
| **The right to withdraw consent** | If consent is your lawful basis for processing personal data (over and above ethical consent being required) then data subjects must be able to withdraw consent as easily as they gave it, and at any time for as long as the personal data exists, even after publication or aggregation. |

### **Exemptions for academic purposes**

If the processing is being carried out with a view to publication, **and** we reasonably believe that the publication of the material would be in the public interest, **and** some of the provisions of the GDPR would be incompatible with the academic purpose of the research, then we could consider not applying those incompatible provisions in particular circumstances. (DPA2018 Sch 2 part 5 based on GDPR art 85(2)). Please contact the information rights team if you believe this would be relevant to your research activities.

### **Checklist:**

* You carry out a DPIA/ checklist and register your data on the IAR
* Privacy notice / participant information sheet
* Appropriate consent form
* Research will not cause damage or distress
* Research must not make decisions about individuals unless for the purposes of approved medical research
* The processing is necessary for the research (GDPR Article 89 and DPA 2018 section 19)
* You should give people the opportunity to agree to participate only in certain areas of research or parts of research projects (Recital 30).
* If processing special category data, ensure the research is in the public interest
* Where possible, inform data subjects about further processing of their data, and take account of consents given
* You only collect personal data you actually need
* Wherever possible, you pseudonymise or anonymise data
* Where necessary, you keep personal data up to date
* You delete personal data which is no longer required
* You have a contract or agreement with all partners and any individuals or organisations you are transferring personal data or pseudonymised data to
* You have identified if any personal data will be transferred or stored outside the EEA, and have appropriate contracts or other safeguards in place
* You have written documents directed at children appropriately, and considered ethical concerns relating to vulnerable research participants
* You have considered how you would meet data subject rights

## **Useful links**

<http://www.open.ac.uk/research/ethics/human-research>

Library and research data management <http://www.open.ac.uk/library-research-support/research-data-management/ethics-and-data-protection>

 Jisc webinar<https://www.jisc.ac.uk/>

1. (The accepted definition of scientific or historical research appears to be the research methods used rather than the subject matter of the research.) Recital 159:… the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. 3In addition, it should take into account the Union’s objective under Article 179(1) TFEU of achieving a European Research Area. 4Scientific research purposes should also include studies conducted in the public interest in the area of public health. 5To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes [↑](#footnote-ref-2)