Data Protection Guidance for UWE Bristol students

Purpose

This guidance is intended for students undertaking research at Undergraduate and Postgraduate taught level that involves the collection and processing of personal data as part of their programme of study at UWE Bristol.

If you are carrying out research for any other purpose than stated above and/or at any other level of study, **do not use** this guidance and refer to the Research governance guidance for Research data management on UWE's website.

Guidance scope

The UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018 (the DPA) protect the rights of individuals when you process personal data about them which includes collecting, storing and disposing of data.

Although there are a number of definitions associated with personal data, for the purposes of this guidance, it is appropriate to assume that personal data is any information that relates to an identified or identifiable individual. This includes any opinion that may be expressed by or about the individual.

Complying with Data Protection Law as an UWE Bristol student

In most circumstances, you (with the appropriate support of the University and your supervisor) are responsible for ensuring that your research complies with the UK GDPR and the DPA. If you follow all relevant guidance, supported by your supervisor, it is extremely unlikely there will be a significant data protection related incident. However, if one does occur, with possible related consequences, UWE will support you by minimising any potential impact.

The GDPR Data Protection Principles

The GDPR is based on seven data protection principles which say that personal data must be:

Processed lawfully, fairly and in a transparent manner

You should tell people why you are collecting their data, how you will use it and who you will be sharing it with (i.e. only the University). Ensure you gain and record their explicit written consent before they participate in your research study.

Further guidance on this data protection principle can be found here

Collected for specified, explicit and legitimate purposes

The personal data that you collect should only be used for the specific purposes (that you have informed the individual of before they participate) relevant to your research and you should not use their personal data in any other way.

Further guidance on this data protection principle can be found here

Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

The personal data you decide to collect should be adequate, relevant and limited to only the data required to support your research study.

Further guidance on this data protection principle can be found here

Accurate and, where necessary, kept up to date

You should ensure that the personal data you collect is accurate and kept up to date if necessary.

Further guidance on this data protection principle can be found here

Kept for no longer than is necessary for the purposes for which it is processed

You should delete and securely dispose of all personal data you have processed when it is no longer needed for the purposes of your research and/or to validate your research results.

Further guidance on this data protection principle can be found here

Processed in a way that ensures it is appropriately secure

You should take appropriate measures to reduce the risks of unlawful or unauthorised access to your research data. You can find some helpful information and guidance on this data protection principle via the Information Security Toolkit however please be mindful that the target audience for this specific guidance is University employees.

Further guidance on this data protection principle can be found here

Be accountable for what you do with personal data

You should take responsibility for what you do with personal data and be able to demonstrate how you comply with the other data protection principles

Further guidance on this data protection principle can be found here

Steps you can take to assist you with data protection compliance

You should complete an initial risk assessment of your proposed research project and share this with your supervisor. Specifically, the risk assessment should take account of the volume of personal data to be collected as well as its sensitivity and whether it includes special category data in determining the outcome and any follow-up approach you decide to take.

You should always consider the possibility/viability of using anonymised data at source/collection as a preferred method of mitigating risks. Truly anonymised data falls outside the UK GDPR framework.

Once you have discussed your risk assessment with your supervisor and you are comfortable proceeding with your project, the following is guidance to consider in helping you manage your work in the data protection area. The key steps you can take in working towards GDPR and DPA compliance for your research project include the following, though there may be others:

1. Document what personal data you need to collect to enable you to complete your research project. Share this with your supervisor so this can form part of all discussions with them.

2. Give a clear written explanation to potential participants of what you are going to do with their data so they can make an informed decision on whether or not to participate in your research study (see template documentation and ethical considerations at the end of this document).

3. Do not collect or keep data that is not necessary for your research. Anonymise data where possible by removing names and other identifying information.

4. Ensure that all personal data, especially qualitative data, for example the participants' views given during conversation and/or an interview, is recorded accurately. If you are unsure of its accuracy,

clarify what you have recorded with the participant to check that they agree with what you have collected.

5. If participants later approach you to request that you update or delete data you have collected for your research project, ensure you follow the relevant ethics procedures in relation to this request.

6. Store personal data securely. For example, you can use UWE OneDrive to assist you with this. Where you need to temporarily store it (for example on a recording device), one measure you can take is to encrypt your device that you are using to store participants personal data. Always delete the data from the recording device as soon as the data has been transferred to your secure method (e.g. OneDrive). You can find some helpful information and guidance on this data protection principle via the Information Security Toolkit however please be mindful the target audience for this specific guidance is University employees.

7. Do not inappropriately share any of your participants' personal data.

8. Securely dispose of all personal data when it is no longer necessary for your research. It is generally considered that all non-anonymised research data you have collected should be disposed of after you have received official confirmation of your award/marks from the University.

Template documentation

- Privacy Notice template for student research (can be found here)

International Research

If you are collecting personal data for your research project in any other country than the UK, please be aware that as well as the requirements to adhere to all guidance made available to you by UWE Bristol, you will also need to adhere to the laws applicable in the country you are conducting your research.

Ethical requirements

In addition to this guidance which relates to data protection (rather than ethics), how you manage personal data while undertaking your research project, will also be governed by the University's Research Ethics Policy and Procedures which must be complied with. In the data protection context please be specifically mindful of the following, which will need to be included as part of the required ethical approval process:

- Participant Information Sheet; and
- Fully Informed Research Participant Consent

Need more advice?

If you have any concerns regarding data protection, please discuss these with your supervisor.

Other relevant links

1. ICO Guide to data protection
2. UWE Information Security Toolkit

V.2: This guidance document was Issued in April 2023 and will be subject to regular review by UWE's Data Protection Office and is scheduled for formal review in April 2024.