

Research at UoM

The University of Manchester (We) conducts research to the highest standards of research integrity to ensure it is both beneficial and enriches higher learning. As stated in our [University Charter](#) our research outcomes are in the public interest. As part of our commitment to research integrity, we follow the General Data Protection Regulation (UK GDPR), the UK Data Protection Act 2018 (DPA) and in the case of health and care research, the [UK Policy Framework for Health and Social Care Research](#).

We promise to respect the confidentiality and sensitivity of the personal information that you provide to us, that we get from other organisations, and that we share with other collaborating organisations (such as other Universities or our research funders). We will tell you how we will use your information, how we will keep it safe and who it will be shared with. We commit to keeping your personal information secure and will not use it to contact you for any other purpose unless you have agreed to this.

Research has a special status under UK GDPR. Research conducted by our staff and postgraduate research students (those studying for a PhD or Masters in Philosophy) is defined as making an original contribution to knowledge which is published in order to share that knowledge.

Research projects may also be conducted by undergraduate and taught postgraduate (Masters in Arts/Science etc.) students to fulfil the requirements of their programme of study. Although these projects are not intended to make an original contribution to knowledge, nor are they usually published, they are essential to the student's education and are therefore included under our definition of research.

We are usually the Data Controller for research studies. This means that we will decide how your personal information is created, collected, used, shared, archived and deleted (processed). When we do this we will ensure that we collect only what is necessary for the project and that you have agreed to this. If any other organisation will make decisions about your information, this will be made clear in the participant information sheet provided to you.

If more than one organisation work together on a project, there may be two or more Data Controllers for a specific project. If this happens, the organisations will have agreements in place which outline their responsibilities and details of this will be made clear in the Participant Information Sheet, provided to you.

Information about you

‘Personal data’ means any information which can identify you. It can include information such as your name, gender, date of birth, address/postcode or other information such as your opinions or thoughts. It can also include information which makes it possible to identify you, even if your name has been removed (such as quotes or social media postings).

We will only ever collect personal information that is appropriate and necessary for the specific research project being conducted. The specific information that we will collect about you will be listed in the Participant Information Sheet, given to you by the research team.

We may process some information about you that is considered to be ‘sensitive’ and this is called ‘special category’ personal data. This includes, but is not limited to, information such as your ethnicity, sexual orientation, gender identity, religious beliefs, details about your health or past criminal convictions. These types of personal information require additional protections, particularly in relation to sharing, which the University ensures are in place.

Under UK GDPR we must have special safeguards in place to help protect your rights and freedoms when using your personal information and these are:

- Policies and procedures that tell our staff and students how to collect and use your information safely.
- Training which ensures our staff and students understand the importance of data protection and how to protect your data.
- Security standards and technical measures that ensure your information is stored safely and securely.
- All research projects involving personal data are scrutinised and approved by a research ethics committee in line with University policies and procedures.
- Contracts with companies or individuals not associated with the University have confidentiality clauses to set out each party’s responsibilities for protecting your information.
- We carry out data protection impact assessments on high risk projects to ensure that your privacy, rights as an individual or freedoms are not affected.
- If we use collaborators outside of Europe, we will ensure that they have adequate data protection laws or are part of privacy and security schemes such as the privacy shield in the US.

In addition to the above University safeguards the UK GDPR and the DPA also require us to meet the following standards when we conduct research with your personal information:

- (a) the research will not cause damage or distress to someone (e.g., physical harm, financial loss or psychological pain).
- (b) the research is not carried out in order to do or decide something in relation to an individual person, unless the processing is for medical research approved by a research ethics committee.

- (c) the Data Controller has technical and organisational safeguards in place (e.g. appropriate staff training and security measures).
- (d) if processing a special category of data, this must be subject to a further public interest test to make sure this particularly sensitive information is required to meet the research objectives.

The Legal Part

Data protection law requires us to have a valid legal reason to process and use personal data about you. This is often called a 'legal basis'. U K GDPR requires us to be explicit with you about the legal basis upon which we rely in order to process information about you.

For research the legal reason is *"Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"* (Article 6 of GDPR):

For sensitive information the legal reason is: *"the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes... 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"*. (Article 9 of GDPR).

When research involves criminal convictions, the legal reason is listed in Schedule 1 of the Data Protection Act 2018 which requires that special safeguards are in place.

Where we need to rely on a different legal reason, such as consent, this will be listed in the Participant Information Sheet provided to you. In clinical trials or medical studies, for example, we may use the following reason:

- *"Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards"*.

We may also use your personal information for additional research purposes, such as other analysis or future projects on the same research topics. This is known as a secondary use or purpose.

If we want to do this it will be explained to you in the Participant Information Sheet and we will ensure that your information will not be used in ways which might have a direct impact on you (such as damage or distress) or will lead to decisions being made about you.

Sharing your information

Your personal information will be kept confidential at all times and researchers are asked to de-identify it (anonymise), pseudonymise (remove any information which can identify you such as your name and replace this with a unique code or key) or delete it as soon as possible. However in some cases it may not be possible to de-identify your information as it is necessary in order to achieve the aims of the research. If this is the case you will be informed of this in the Participant Information Sheet.

Your personal information as well as any de-identified information will only be shared with members of the research team in order to conduct the project. If they need to share your information with anyone else including anyone outside of the European Economic Area (which includes all countries of the European Union as well as Norway, Iceland and Liechtenstein), you will be told who they are and why this is the case in the Participant Information Sheet.

We also sometimes use products or services provided by third parties who carry out a task on our behalf, such as Dropbox for Business, which is used for sharing research data. These third parties are known as data processors and when we use them we have agreements in place to ensure your information is kept safe. This does not always mean that they access your information but if they do this will be outlined in the Participant Information Sheet. As Data Controller, we will always remain responsible for keeping your information safe throughout the research.

We will only keep your personal information for as long as necessary to complete the aims of the research. However, some personal information (including signed records of consent) will be kept for a minimum amount of time as required by external funders or our policies and procedures. You can read more about how long we will keep this information for in our [retention schedule](#). The Participant Information Sheet will state how long your personal information will be kept and for what purpose.

For some research projects, your de-identified or pseudonymised information will be kept after the project has ended, placed into a data repository/online archive for sharing with other researchers or used in future research. If the researchers would like to do this with your information you will be told in the Participant Information Sheet.

When using research repositories, researchers are often required to upload their supporting or underlying data which may be identifiable or sensitive. The repositories have technical controls in place to ensure that only authorised individuals can access the information.

NHS LOGIN

Please note that if you access our service using your NHS login details, the identity verification services are managed by NHS Digital. NHS Digital is the controller for any personal information you provided to NHS Digital to get an NHS login account and verify your identity, and uses that

personal information solely for that single purpose. For this personal information, our role is a “processor” only and we must act under the instructions provided by NHS Digital (as the “controller”) when verifying your identity. To see NHS Digital’s Privacy Notice and Terms and Conditions, please click here <https://access.login.nhs.uk/terms-and-conditions>. This restriction does not apply to the personal information you provide to us separately.

Your rights

By law you have rights in relation to the personal information we hold about you. These include the right to:

- See the information/receive a copy of the information;
- Correct any inaccurate information;
- Have any information deleted;
- Limit or raise concerns to our processing of the information;
- Move your information (“portability”).

These rights only apply to your information before it is anonymised as once this happens we can no longer identify your specific information. Sometimes your rights may be limited if it would prevent or delay the research. If this happens you will be informed and have the right to complain about this to the Information Commissioner.

If you have any questions about how your personal information is used, or wish to exercise any of your rights, please consult the [University’s data protection webpages](#). If you need further assistance, please contact the University’s Data Protection Officer, Tony Brown (dataprotection@manchester.ac.uk) or write to:

The Data Protection Officer
Information Governance Office, Christie Building
University of Manchester, Oxford Road
Manchester M13 9PL

If you are not happy with the way your information is being handled, or with the response received from us, you have the right to lodge a complaint with the Information Commissioner’s Office at Wycliffe House, Water Lane, Wilmslow, SK9 5AF (<https://ico.org.uk/>).