Privacy Notice for Research Participants

Edinburgh Napier University, as the Data Controller, is providing you with this information in order for us to comply with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018, which require us to tell you what we do with your personal information.

Introduction/Purposes
This privacy notice deals with personal data provided for the purposes of research only.

Edinburgh Napier University ("We") conducts research to the highest standards of research integrity to ensure it is both beneficial (generally) and enriches higher learning. We 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 commit to protecting your personal information secure and complying with the legislation.

Research has a special status under Data Protection legislation. Research conducted by our staff and postgraduate research students 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 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 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.

Who is the Data Controller?
The University is 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 make clear in the Participant Information Sheet, provided to you.

What personal data is collected from research participants?
The specific information that we will collect about you will be listed in the Participant Information Sheet, given to you by the researcher/s. This data may include your name, gender, date of birth, contact details, online and location identifiers, your opinions or comments/quotes or social media postings. It may also include sensitive (special category) data, such as your ethnicity, sexual orientation, gender identity, religious beliefs, biometric or genetic data, details about your health or past criminal convictions, etc.. Data collected should only be that which is appropriate and necessary for the specific research project being conducted.

Who is research data shared with?
Your personal information will be kept confidential at all times and researchers are required to pseudonymise/codify (remove any information which can identify you such as your name and replace this with a unique code or key), de-identify (anonymise), 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. Where researchers wish to use any information that would identify you, specific consent will be sought.

Your personal information as well as any de-identified information may be shared with:

- The research project team who are authorised to work on the project and access the information - this may include University employees and authorised collaborators at other organisations.
- Where a student is undertaking the research the data may be shared with their supervisors.
- Auditors, where research audits require access to the data.
- Where there are complaints or data subject rights requests Governance Services, the Research and Innovation Office, Ethics Committee members, appointed investigators, etc. may need access to the data.

If researchers need to share your information with anyone else including anyone outside of the European Economic Area, 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 processing on our behalf or provide services or data storage/processing facilities. 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.

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.

The University undertakes to maintain your information securely and will restrict access to employees, our professional advisers, authorised agents and contractors on a strictly need to know basis. We will only disclose your data to external third parties (other than any specified above) where there is a justified purpose and we:

- Have your consent
- Are required to do so under a statutory or legal obligation, or
- Are permitted to do so by Data Protection legislation.

The University NEVER sells personal data to third parties.

Your anonymised data will be included in the resulting research output and may form part of a research publication, conference presentation or public talk.

What is the legal basis for processing?

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'. 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 basis the University relies on is Article 6(1)(e): for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller, namely the University's Statutory Instruments: "for the objects of …carrying out research".

Where sensitive personal data is being processed the additional bases from Article 9(2)(j) 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*".

When research involves criminal convictions, the University relies on the legal basis as provided for by Schedule 1, Part 1, Section 4 of the Data Protection Act 2018, and researchers must ensure that special safeguards, as required by the legislation, are in place.

Where we need to rely on a different legal reason, 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:
GDPR Article 9(2)(h): "*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*".

Where anonymous data is provided by other organisations for research purposes this is not covered by data protection legislation, however researchers will submit the data to rigorous checks to ensure it can never be reconstituted with other data to identify individuals. Due care will also be taken with research outputs to ensure they are disaggregated to the extent possible to ensure anonymity.

How are we collecting this information?
Researchers may collect participant information in a number or ways, including: in person, online/electronically, from or via a third party, etc.

How long is your information kept?
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.

Further information can be found online at: https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsRetentionSchedules.aspx

How secure is your information?
For services provided locally by Information Services, information is stored on servers located in secure University datacentres. These datacentres are resilient and feature access controls, environmental monitoring, backup power supplies and redundant hardware. Information on these servers is backed up regularly. The University has various data protection and information security policies and procedures to ensure that appropriate organisational and technical measures are in place to protect the privacy of your personal data. The University makes use of a number of third party, including "cloud", services for information storage and processing. Through procurement and contract management procedures the University ensures that these services have appropriate organisational and technical measures to comply with data protection legislation. The University is Cyber Essentials Plus accredited.

Where researchers use systems and services not provided as standard through Information Services they are required to ensure that Data Protection and Information Services checks have been completed and approved by Governance Services and Information Services, which are likely to include Privacy Impact Assessments, and that the necessary Data Sharing/Processing Agreements are in place.

Researchers must provide assurances in their Participant Information Sheets as to the local measures they are taking e.g. data is pseudonymised/anonymised, password protected/access restricted/under lock and key, kept in University/University approved systems, etc.

Who keeps your information updated?
Researchers rely on participants to advise them of any personal data which needs to be updated.

Will your information be used for any automated decision making or profiling?
The researcher/s will advise in the Participant Information. If the answer is 'yes' meaningful information about the logic involved, significance and envisaged consequences of such processing to must be provided.

Is information transferred to a third country? Outside the EEA and not included in the adequate countries list.
The researcher/s will advise in the Participant Information.

Safeguards
Under Data Protection legislation 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 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 Data Protection legislation also requires 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.

What are 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 or contact the University's Data Protection Officer at dataprotection@napier.ac.uk
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/).

For more information please see: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx

The University gratefully acknowledges the University of Manchester's permission to use and adapt its materials.