Research and Data Protection (updated May 2019)

This guidance is based on the requirements of the EU General Data Protection Regulation (GDPR) 2016 and UK Data Protection Act 2018 which came into force in May 2018.

Data protection legislation is regulated by the UK Information Commissioner's Office (ICO) and reference to them and links to their guidance online may be included below.

The GDPR states: "Personal data should be processed *only* if the purpose of the processing could not reasonably be fulfilled by other means" (Recital 39) e.g. if you *don't* need to process personal data then ***don't*** – use anonymised data wherever possible!

The GDPR allows for "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" (Article 89), however the research must comply with the legislation and **data protection principles** and is subject to **appropriate safeguards** for the rights and freedoms of data subjects (research participants) being in place. At the heart of these safeguards is **data minimisation** – using the absolute minimum data required to achieve the research aims and objectives in all/any processing done, from collection, through manipulation to destruction/archiving and pseudonymising or anonymising it wherever possible. Researchers must ensure that **technical and organisational measures** are in place to protect personal data and privacy. Ideally, if the research can be done with **anonymised data**, then this should be done as early as possible. Anonymised data is that which can never be reconstituted to identify an individual. If anonymisation is not possible researchers must **pseudonymise** or **encrypt** the personal data wherever possible.

This guidance uses the terms data subject, individual and research participant interchangeably and with the same meaning. Employed researchers must read the University's Staff Privacy Notice for information relating to the processing of their personal data.

Appropriate safeguards for the rights and freedoms of individuals, as noted within the legislation (Recital 156) are:

a) Procedures to allow individuals to exercise their rights under the legislation
b) Appropriate organisational and technical measures in place to maintain the integrity and confidentiality of the personal data being processed
c) Compliance with other relevant legislation e.g. that for clinical trials

Additionally, following the advice given in this guidance to ensure compliance with the legislation will provide the appropriate protection and safeguards.

Contents

1) Definitions of personal data

GDPR expands the definitions of personal data (from that used previously) to include:

- Online identifiers
- Location data
- IP addresses
- Cookie IDs
- Genetic data*
- Biometric data*

This means that the additional protections required by the legislation for personal data must now be applied to these classes of data.

*Data classed as “sensitive” personal data previously is now referred to as “special categories” of personal data – this data requires a higher level of care which may include further restricted access, additional security and shorter retention periods.

The definition (Article 4(1)) is: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data (Article 9) requiring an additional legal basis for processing include: ‘personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,

data concerning health or data concerning a natural person's sex life or sexual orientation'.
Criminal convictions data will be processed under the Data Protection Act 2018 Schedule 1 Part 1 Section 4 (derogations allowed in Art 10 GDPR), however currently this is not possible as the University does not have a Policy in place for processing criminal convictions data for research which is specifically required by the Data Protection Act 2018.

2) Terminology definitions

Anonymised data is where personal data or personally identifiable information (data from which an individual can be identified) is removed and the data can never be reconstituted to identify an individual. The context of the information must be taken into account e.g. a study on a rare disease where only one individual in a postcode suffers from the disease may allow identification were the figure of 1 reported against the full postcode. The ICO's guidance on anonymisation is available here: https://ico.org.uk/media/1061/anonymisation-code.pdf. Article 26 refers.

Encryption is where data is converted into code using an algorithm and can be reconstituted or read where the encryption key (similar to a password) is used.

Pseudonymisation means that identifiers in information are replaced with pseudonyms, but the identifying information is kept separately and the data can be reconstituted if required. Article 26 refers.

3) Data protection principles

Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner – this means the researcher or organisation must have a **legal basis** for processing and data subjects **must be given** a **privacy notice** which tells them what is being done with their personal data. Data subjects have the right to receive a privacy notice. If you cannot explain what you are doing with the data then it is unlikely that it is being processed lawfully, unless an exemption applies.

(b) Processed for specified, explicit and legitimate **purposes** and not further processed in a manner which is incompatible with those purposes. However, research is not considered incompatible with the initial purposes as long as it is aligned to those purposes and not used for a different area of research which the data subject would not expect it to be used for.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. As mentioned above data minimisation is key.

(d) **Accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are corrected or erased without delay.

(e) Kept for no longer than necessary for the purposes for which it was collected. However, it can be kept longer for research purposes as long as there are appropriate safeguards, technical and organisational measures in place to protect the data and data subjects. Data **retention period/s** must be decided

and recorded at the beginning of a project and measures put in place for the data to be destroyed if the primary research leaves the University.

(f) Processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures to maintain the integrity and confidentiality of the data.

Additionally,

(g) The researcher is responsible for keeping records of what personal data is collected and how it is processed to **demonstrate compliance** with the legislation.

(h) The data must be processed in line with individual's **rights**.

(i) The data must not be transferred to **countries outwith the EEA** without adequate protection.

4) Legal Basis for processing

The University is the Data Controller for research done under the auspices of the University. Both staff and students are therefore required to adhere to the stipulated requirements following the University's Data Protection Policy and Code of Practice and completing an oath of confidentiality (unless employed by the University where this is included in the contract of employment), data protection checklist (Appendix 2) or Privacy Impact Assessment, Privacy Notice (copy to be provided to all research participants) and Data Sharing/Processing Agreements (if personal data is shared with 3rd parties).

Where the University is the controller the legal bases for processing is: *"Processing is necessary in the exercise of **official authority vested in the controller**"* (Article 6 refers)(commonly known as "public task"). The University's Statutory Instruments refer: "for the objects of providing education, carrying out *research* and promoting teaching, *research* and general scholarship".

Where **sensitive** (special category) personal data is used a condition from Article 9 (DPA Schedule 1, Part 1, Section 4) is required and this is Art 9(2)(j): *"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 interests of the data subject"*.

Use of this basis must be accompanied by explanations of:

a) How the use of data is proportionate to the aim pursued
b) What suitable and specific measures are in place to safeguard the fundamental rights and interests of the participants, e.g.:
    i. The technical and organisational measures in place, particularly with regard to data minimisation e.g. pseudonymisation
    ii. Anonymised data is used wherever possible
    iii. How individuals can exercise their rights, where allowed and not exempt under the DPA 2018, that is, exercising those

rights would severely impair the achievement of the research purposes (DPA Sch 2 Pt 6)

iv. No measures will be taken, or decisions made, about individuals unless it is for the purposes of approved medical research*

v. Processing will not, or is not likely to, cause substantial damage or distress to individuals

* See Section 9 for a list of bodies which can approve medical research.

5) Transparency and Privacy Notices

Where personal data is collected directly from research participants a privacy notice must be provided at the time of collection. A sample template is attached at **Appendix 1**. This information should be drawn from the project's data management plan, however, the details of the security arrangements in place to protect the personal data from loss, damage or unlawful disclosure should be fully detailed in the data management plan with an extract provided for participants, should the disclosure of full details present a risk to the security of the data.

Where the personal data has been collected by a third party, the researcher must, if possible, present the data subjects with a privacy notice within 30 days of receiving their personal data (article 14), unless the data subjects already have the information or it would involve a disproportionate effort (particularly for research) or is impossible.

There may be instances, e.g. secondary use of data from the NHS, where it is not possible. Researchers must check what is included in privacy notices given to participants and ensure the research is not incompatible with the purposes for which the data was collected.

Where the provision of privacy notices for research projects proves to be impossible or requires disproportionate effort e.g. when using older data, the GDPR makes allowance for this, however, researchers must keep a record of the reasons they were not able to provide privacy notices. Recital 62 refers.

Where researchers are conducting research in a public place e.g. a transport survey, where the provision of privacy notices to individuals is not appropriate or possible, researchers must consider placing a privacy notice poster/s in the general vicinity of the research being undertaken, where possible, to inform the public.

6) Purpose

When stating the purpose for processing researchers should cover all processing activities carried out for the same purpose or purposes. Multiple purposes can be included in one privacy notice. If researchers are obtaining personal data from research participants for one research project only and are unlikely to re-use that data then the stated purpose can only include information about that one project, however, researchers must consider if there will be any future re-use of the personal data for similar research projects and if there is any likelihood that this will be the

case then they should structure the “purpose” statement appropriately to inform the data subject of this.

Article 33 allows a vaguer purpose for processing where research is concerned and states: “It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.”

If this is the case then you must seek consent for the broader area of research and you must not then go on to use the data for a different area of research without first seeking fresh consent (unless another legal basis for processing exists).

7) Retention

The retention period/s for personal data must be defined at the outset of the project and this must be clear from the cover paperwork, in the data management plan, and wherever possible in the metadata of both paper/physical and electronic records.

Where Researchers need to comply with external funding body requirements this will determine the retention period.

Where there are no external requirements researchers can take cognisance of accrediting body requirements, legislative requirements and University business requirements.

Researchers must take into account that certain personal data where there is a higher degree of privacy invasion or risk of harm to an individual, e.g. special category, audio/visual recordings of participant data, etc. will be held for a shorter time period than other less sensitive data e.g. anonymised transcripts, however, researchers must consider the possibility of data being required to evidence the veracity of the research.

The legislation says data must be kept for no longer than necessary for the purposes for which it was collected and as the research project is the purpose, researchers must consider how long it is absolutely necessary to keep personal data if there are no external requirements, for example, an undergraduate dissertation for the purposes of a degree award where the researcher has no intention of continuing with research after graduation is likely to have a very short retention period for any personal data collected (no external funder or professional body requirements), whereas a longitudinal health study tracking participants over several years is likely to have a much longer retention period as personal data is required to continue the research (also likely to be subject to external funder/body requirements).

The retention period must start from a defined ‘action’ or event, which, for research, is usually the date that the project closes or the research is submitted/published. Researchers need to take into account the practicalities of how this will be dealt with,

depending on the 'system' used to manage the data and who will be responsible for destroying the data in future (particularly if there is a long retention period) – to this end it may be necessary to use an alternative event like the date of creation or collection of the data.

8) Disposal

All personal data, whether in hard copy (paper or other) or electronic must be confidentially disposed of. Guidance is available online using the following link: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/DestructionofPersonalData.aspx

9) Safeguards

Safeguards are measures which are put in place to protect the rights and freedoms of individuals whose personal data is being processed (data subjects/research participants/etc.) and include the following:

1) **Organisational and technical measures for data security**

a) Organisational measures:

1) Training: Researchers handling personal data must complete data protection training. Dependent on the type of researcher e.g. employed or student, the University makes training available in a number of ways. The supervisor or principal investigator must ensure appropriate training is provided to ensure researchers understand their responsibilities with regard to the legislation and to individuals whose data is being used for the research project.
2) Confidentiality: All researchers processing personal data must sign an oath of confidentiality. A template is available online using the following link: https://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/Oaths.aspx
3) Policies: The University has a Data Protection Policy Statement and Code of Practice, employed researchers must ensure they are aware of their responsibilities under this and other allied policies e.g. Information Security and Research Data Management policies.

b) Technical measures:

1) The University provides a secure electronic network- researchers must ensure that research data is kept either on the X: Drive (employed researchers) or F: Drive. Staff/paid researchers must not use the H: Drive. Not only are these areas secure, but are also backed up on a daily basis to reduce the risk of loss of data. Where the University electronic network or services provided by the University Information Services team is used to process personal data the following statement can be given in the "security" section of the privacy notice (full details in the data management plan): "*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 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."
This statement can **not** be used where external/3rd party systems/apps are used – a separate security check and statement is required.

2) 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 or your personal data.
3) Researchers must ensure that they apply local security measures which they have control over e.g.
    a. Do not label files containing personal data with the research participant's name. You should give each participant a unique number and keep a 'key' (list) linking those numbers to research participant's names in a secure password protected file to which only you have access, then use that unique number on all the other data that you collect. This means that the only way to link personal data to research data is by using the 'key'.
    b. Password protecting electronic files containing personal data
    c. Restricting access to electronic folders/sites/storage areas. Employed researchers must make appropriate arrangements with their supervisor for alternative access in the event they are absent e.g. data should not be inaccessible or "lost".
    d. Any transfer of data must be secure. Sending personal data by email must be avoided wherever possible, however, if unavoidable the data should be included in a password protected document (password provided to the recipient separately) and encrypted if sent externally (out of the University). The University provides a free encryption service to employees and associates. Emails send within the University network e.g. from an @napier.ac.uk to @napier.ac.uk email addresses is secure, BUT researchers must ensure emails are sent to the correct recipient – the Microsoft 'autofill' address function makes it easy to select the wrong email address. Researchers should use Sharepoint, if possible, where any transfer of personal data is necessary.
    e. Drop-box is NOT a University approved storage facility. Personal data must NOT be stored in Drop-box. The University is working to provide an alternative, Office 365/One Drive, in 2019.
    f. Storing data on portable devices should be avoided wherever possible, however, if it is unavoidable portable devices must be encrypted. The University provides a data encryption service. If using personal devices (laptop, tablet, phone, etc.) to access the University network researchers must ensure the device has up-to-date anti-virus software. The University provides a free anti-virus solution and facilities to log into the network securely. Guidance on mobile device security is available online here: https://staff.napier.ac.uk/services/cit/infosecurity/Pages/Mobile-Device-Security.aspx. Storing personal data on a personal device means that it will need to be thoroughly and professionally "wiped" before it can be

disposed of, therefore it is recommended that 3rd party/research participant personal data is NOT processed on a personal device.

g. Keep your passwords secure and never share your login details.
h. If using 3rd party products, cloud services, etc. not provided by the University due diligence relating to the security of the product and its suitability for processing personal data must be done during the procurement exercise or by contacting Information Services.

4) Paper or manual records must be kept securely – the University's Manual and Physical Data Security Policy provides more information.

2) Rights

Researchers must ensure appropriate measures are taken for them to allow individuals to exercise their rights, where appropriate, should they wish to do so e.g. data and records management processes and metadata in place to enable specific personal data to be found/retrieved. In the case of research, the ability of individuals to exercise their rights may be affected by the maturity of the project and any measures taken to minimise the processing of personal data. Where the exercising of rights marked * would prevent or seriously impair the achievement of the research purposes they do not apply e.g. can't be exercised (DPA 18 Sch2 Pt 6 S.27).

Data subjects have the following rights:

a) To be informed e.g. receive a privacy notice
b) To access e.g. obtain a copy of their personal data being processed (subject access request) * (Art 15 (1) to (3) confirmation or, and access to, data)
c) To have their data rectified if it is incorrect * (Art 16)
d) To erasure (right to be forgotten) where it is no longer necessary for the purposes, but not where this is likely to render impossible or seriously impair the objectives of a research project
e) To restrict personal data being processed * (Art 18(1))
f) To portability (request a copy of the data provided in a machine readable format)
g) To object to processing in certain circumstances * (Art 21(1))
h) To be notified of their rights
i) Not to be subject to decisions, which affect them as an individual, based on automated processing (only) and profiling activities
j) To be informed if there is a breach of their personal data which will result in a (high) risk to their rights and freedoms (**this is a decision for the Data Protection Officer in Governance and Compliance *only* – in the event of a data breach follow the University's procedure**)

The privacy notice template provides a link to information about rights on the University intranet pages as standard.

The legal basis for processing also affects the application of some rights - the ICO has provided the table below showing when rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

The right to object does not apply where the legal basis for processing is that the research is in the public interest.

10) Exemptions

There is an exemption from the data protection legislation (DPA 2018 Part 2 Ch 3(25) which allows for manual unstructured data used in longstanding historical research which was underway prior to 24/10/1998 to be exempt from Principle 4 (accuracy) and data subject rights to rectification and erasure, as long as the processing is not carried out for the purposes of:

a) For the purposes of measures/decisions to be taken/made about individuals, and
b) In a way that causes, or is likely to cause, substantial damage or distress to individual/s

11) Legislative references

"Approved medical research"
Bodies which can approve medical research for the purposes of the legislation are those as set out in the DPA 2018 Chapter 2(19)(4) as below:

(4) In this section—

"approved medical research" means medical research carried out by a person who has approval to carry out that research from—

(a) a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or

(b) a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—

(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;

(ii) a relevant NHS body;

(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;

(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);

"relevant NHS body" means—

(a) an NHS trust or NHS foundation trust in England,

(b) an NHS trust or Local Health Board in Wales,

(c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,

(d) the Common Services Agency for the Scottish Health Service, or

(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 (c. 1 (N.I.)).

Pseudonymisation and anonymisation

Recital 26 refers: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Purposes and further processing

Recital 50 refers: "The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations."

Privacy notices
Recital 62 refers: "However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration."

Safeguards
Recital 156 refers: "The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing

along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials."

Continued in Recitals 157 to 162