Data Protection Policy

1 Introduction

The University of Northampton is committed to protecting the privacy rights of individuals under data protection legislation and takes its responsibility for handling personal data very seriously. This policy sets out the fundamental requirements which are underpinned by further policies, procedures and more detailed guidance documentation.

2 Scope

This policy applies to all personal data processed by the University for business and research purposes, irrespective of how that personal data is held. It therefore covers personal data held both electronically and on paper files applies to all individuals who process personal data for or on behalf of the University. The University of Northampton processes the personal data of a wide range of individuals including (but not limited to) employees; honorary staff; research subjects; students; contractors and visitors. Additionally, any business function that engages with service providers outside of the University of Northampton must ensure that these providers abide by the same data protection standards.

Definitions:

Before diving into the specific elements of a data protection policy, it is essential to establish clear definitions for key terms and concepts. This will ensure that all stakeholders understand the scope and requirements of the policy. Some important terms to define include:

- **Personal data**: Information relating to living individuals can be identified or identifiable by name, identification number, location data, email, online identifiers etc.
- **Processing**: Operation performed on personal data, such as access, collection, recording, structuring, storage, adaptation, retrieval, destruction, etc.
- **Data controller**: The organisation that determines the purposes and means of the processing of personal data.
- **Data processor**: The organisation that processes personal data on behalf of the data controller.

- **Data subject**: The individual whose personal data is being processed.
- **ICO**: Information Commissioner's Office. The UK's independent body set up to uphold information rights

3 Applicable Laws

This policy applies to personal data processed in accordance with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The policy gives due regard to personal data requirements under other laws and regulations, including but not limited to:

- Human Rights Act 1998
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990

4 Data Protection Principles

The Data Protection Principles are the foundation of data protection law. If properly adhered to, there is very little scope for breaching the applicable laws. All personal data must be processed in accordance with the seven Data Protection Principles below.

- **Lawfulness, fairness, and transparency**: Personal data must be processed in a lawful, fair, and transparent manner, with clear communication to data subjects about how their data is being used
- **Purpose limitation**: Personal data should only be collected for specific, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be viewed as incompatible with the initial purposes
- **Data minimisation**: The collection of personal data should be limited to what is necessary for the intended purpose, and no more

- **Accuracy**: Personal data must be 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 erased, or rectified without delay
- **Storage limitation:** Personal data should not be stored for longer than necessary for the intended purpose. Where Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR to safeguard the rights and freedoms of individuals.
- **Integrity and confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage. Technical security measures include the use of encryption, firewalls and pseudonymisation. Organisational measures include policies and procedures, and data protection impact assessments (DPIAs)
- **Accountability**: Data controllers must be able to demonstrate compliance with the GDPR principles, including having appropriate policies and procedures in place. To meet the requirements of accountability the University as a Data Controller must have in place appropriate technical and organisational measures which include:
    - Adopting and implementing **data protection policies**
    - Taking a **'data protection by design and default'** approach
    - Having **written contracts** and contracts register in place with organisations that process Personal Data on the University's behalf.
    - **Maintaining documentation and a current record** of its processing activities
    - Implementing appropriate **security measures** recording and reporting internally and, where necessary, reporting **Personal Data breaches** to the Information Commissioner's Office (ICO) (Refer to Data Breach Policy)
    - Carrying out **data protection impact assessments** (DPIAs) for uses of Personal Data that are likely to result in high risk to individuals' interests
    - Appointing a **Data Protection Officer** and adhering to relevant **codes of conduct** and signing up to certification schemes

5 Lawful Processing of Data

There must be a lawful basis for processing personal data. Possible lawful bases are:

- **Consent**: The data subject has given their clear and unambiguous consent for the processing of their personal data
- **Contract**: The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject before signing a contract
- **Legal obligation**: The processing is necessary for compliance with a legal obligation to which the data controller is subject
- **Vital interests**: The processing is necessary to protect the vital interests of the data subject or another individual
- **Public interest**: 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 data controller
- **Legitimate interests**: The processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Processing involving a third party takes place only in accordance with the applicable legislation and principles of data protection and will be governed by an agreement or arrangement with the third party in accordance with the legislation and principles

6 Lawful basis for processing special category data

Listed below are the different types of Special Category personal data as categorised by UK GDPR Article 9. This nature of data presents a higher risk to the rights and freedoms of individuals for example, its processing in the wrong hands presents a higher risk of discrimination against an individual.

- Racial or ethnic origin
- Political opinions
- Religious or political beliefs
- Biometric data
- Trade union membership
- Genetic data

- Health
- Sex life
- Sexual orientation

Where Special Category data are processed an additional lawful basis to that for processing personal data must be identified from those below:

a) Explicit consent
b) Employment, social security, and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies (defined as processing in the course of the legitimate activities of a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim. Processing takes place on condition that it relates solely to the member or former members of the body or to persons who have regular contact with it in connection with its purposes and that personal data is not disclosed outside that body without the consent of the data subject)
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research, and statistics (with a basis in law)

If relying on conditions b), h), i) or j), you also need to meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. If you are relying on the substantial public interest condition in GDPR Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. For advice and guidance on applying the lawful bases, contact the Data Protection and Information Governance Team by emailing dpo@northampton.ac.uk.

7 Individual rights

Data protection provides the following rights for individuals. Requests received by the University where individuals are exercising their rights are managed by the Data Protection and Information Governance team and require a response within **one calendar month**. There is no fee for exercising a right in most circumstances, in some cases, an exemption to the right may apply which means

that sometimes the University will not need to provide the information, or part of the information, to the requestor. Some rights set out below are referred to as 'not an absolute right', which means that the University needs to consider the application of an exemption.

- **The right to be informed**
  Individuals have the right to be informed about the collection and use of their Personal Data at the time it is collected from them. They are usually notified through a Privacy Notice and there is a requirement to provide some specific information.

- **The right of access**
  Individuals can request to obtain a copy of the Personal Data held about them along with other supplementary information. This is known as a data subject access right (DSAR) and can be made verbally or in written form.

- **The right to rectification**
  Individuals have the right to have inaccurate Personal Data rectified, or completed if it is incomplete.

- **The right to erasure – ('right to be forgotten')**
  Individuals have the right to have Personal Data erased in certain circumstances. This is not an absolute right.

- **The right to restrict processing**
  Individuals have the right to request a restriction or suppression of their Personal Data in certain circumstances. This is not an absolute right. Where it applies, the University is permitted to store the Personal Data but not use it.

- **The right to data portability**
  This right allows individuals to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without affecting its usability.

- **The right to object**

Individuals have the right to object to the processing of their Personal Data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. However, in other cases where the right applies you may be able to continue processing if you can show you have a compelling reason for doing so.

- **Rights in relation to automated decision making and profiling**
  Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on the individual or similarly significantly affects the individual. An example would be deciding to interview a person based solely on the results of an online aptitude test. This decision has a significant effect since it determines whether or not someone can be considered for the job.

  Profiling means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

It is important that information from central systems such as SITs (the student records system) for example should **not be deleted locally.** This is because at times, information that is intended to be deleted could be falling within the retention schedules in place. Information from these systems is only deleted by IT Services in conjunction with Data Protection and Information Governance team. For data held locally or on stand alone systems a deletion request can be met by authorisation of the relevant manager in consultation with the Data Protection and Information Governance team.

8 Record of Processing Activity (ROPA)

Under UK GDPR Article 30, the University is required to maintain a record of all processing activities under its responsibility. The record must contain:

- Name and contact details of the Controller (University) and where applicable details of the Joint Controller or the Controller's representative.
- Name and contact details of the Data Protection Officer (see below)

- The purposes of the processing
- What personal data is being processed
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has been or will be disclosed including recipients outside the UK or international organisations
- Where applicable, transfers of personal data to a third country or an international organisation. This should include details of that country or international organisation and where relevant documentation of suitable safeguards
- Where possible, the envisaged time limits for erasure of the different categories of data
- Where possible, a general description of the technical and organisational security measures in place
- As well as the above, the ROPA used by the University of Northampton also contains questions to help undertake a preliminary risk assessment for a processing activity (a phase one questionnaire).

It is the responsibility of process owners (whether researchers, academic or professional service staff) who manage or oversee data processing activities to ensure all activities in their control are accurately captured and reflected in the Record of Processing Activities and kept up to date according to the above requirements.

This is an organisational measure which falls under the obligations of the Accountability Principle and is a requirement of Article 30 of the UK GDPR.

The ROPA entry must be completed when a new activity/initiative involving personal data is starting or a new process is being introduced. In cases where a process changes, the original ROPA entry must be reviewed to ensure the changes are captured. This also enables risks to be identified at an early stage.

The ROPA is a description of the University's processing of personal data and does not itself contain personal data. It does not affect individual rights as set out in section 7 of this policy.

9 Basic responsibilities of staff for data security when processing personal data

The University has a legal requirement to ensure that data is held securely Access to and disclosure of personal data must be restricted to those who have a legitimate, authorised purpose and where necessary on a need-to-know basis.

Staff are responsible for using and otherwise processing personal data in compliance with this Policy and operating under the terms of the UK GDPR and Data Protection Act 2018.

All staff are responsible for ensuring that:

- personal information is not disclosed by them either orally or in writing, to any unauthorised third party
- they do not access any personal data which is not necessary for carrying out their work
- personal data in paper format is kept in a secure place when not being
- processed
- personal data on computer should not be accessed or viewed by
- unauthorised staff or students and as such workstations must be locked or password protected when not in use
- where personal data is held on paper, this **should not** be removed from the University
- buildings unless it is via a secured electronic means and with authorisation from Data risk owner(s).
- staff processing personal data for research purposes should include a Data Protection Privacy Notice informing the data subject, in this case a research participant, of as the following:
    - What data is being collected
    - Why the data is being collected
    - The legal basis for processing
    - How long it will be retained for
    - Rights of the participants
    - Who to contact when they need to exercise their rights or complain as a participant. To complain about the research itself, the appropriate contact will be the team/person conducting the research To enforce their rights, the contact is the Data

protection and Information Governance team. Data subject can also escalate to the Information Commissioner's Office (ICO).

If in doubt, please contact the Data protection and Information Governance Team for advice at dpo@northampton.ac.uk.

10 Responsibilities of students when processing personal data

Students may need to process personal information for project or research purposes which include the collection and processing of personal data. This can include activities such as questionnaires, surveys, and focus groups where participants are interviewed. In carrying out these activities, students have the same responsibilities as staff as stated in section 9.

Students processing personal data for projects or research must ensure that data subjects receive a Data Protection Privacy notice including the same information set out in section 9 above. If students are processing personal data, then they must obtain appropriate approval from their lecturer or supervisor and should be aware that they may also need ethics approval.

11 How to make international transfers in compliance with the UK GDPR

Consider whether you can achieve your aim without sending personal data. If not, can you make personal data anonymous which means an individual can never be identified from the information being transferred, even when that information is combined with other information available to the receiver? Anonymised data is no longer classified as personal data and the restrictions will not apply.

It is particularly important to ensure compliance if personal data is being transferred outside the UK/EEA, as different jurisdictions have varying data protection laws. Where the service provider is not within the UK/EEA, a review will be conducted through a Data Protection Impact assessment (DPIA), which will be completed by the stakeholder. This will review the risks of the processing.

Personal data transfers can be made outside the UK by working through the following questions in order. If by the last question you are still unable to make the restricted transfer, then it will be in breach of the UK GDPR.

11.1 Is the restricted transfer covered by Adequacy Regulations?

A restricted transfer can be made where the receiver is outside the UK/EEA provided that the location or organisation is covered by a UK adequacy decision made under the UK adequacy regulations. These regulations set out in law that the legal framework where the receiver is located has been assessed as providing adequate protection for individuals' rights and freedoms in relation to their personal data. This allows the restricted transfer to take place safely and legally without any additional measures being required.

Under provisional arrangements UK adequacy regulations include the EEA and all countries, territories and international organisations covered by European Commission (EC) adequacy decisions. This is currently under review as at 30 January 2024 as the Data Protection and Digital information Bill is still being reviewed in the House of Commons.

Up to date information on adequacy regulations and decisions that have been made can be found at the following ICO website link on International Transfers and information about the UK-US data privacy framework.

11.2 Restrictions on international transfers

The UK GDPR restricts transfers of personal data to countries or international organisations outside the UK or the protection of the UK GDPR. Transfers cannot be made unless the personal data rights of the individuals are protected, or an exception applies.

Transfer of personal data is restricted if:

- The UK GDPR applies to the processing of the personal data you are transferring.
- You are sending personal data, or making it accessible to a receiver to which the UK GDPR will not apply in relation to their processing of the personal data; and
- The receiver is legally distinct from the University as it is a separate

company, organisation or individual.

If you are sending personal data to someone employed by the University this is not a restricted transfer.

11.3 Is the restricted transfer covered by appropriate safeguards?

Where there is no adequacy regulation for the country, territory or sector proposed for a restricted transfer, transfer can still proceed subject to meeting appropriate safeguards listed in the UK GDPR. Each ensures that both you and the receiver of the restricted transfer are legally required to protect individuals' rights and freedoms in respect of their personal data.

Before relying on an appropriate safeguard to make a restricted transfer, a **Transfer impact assessment** (TIA) to identify risk needs to be undertaken. This is to assess the protections contained within that appropriate safeguard and the destination country (including laws governing public authority access to the data). This is to help ensure a level of protection equivalent to that under the UK data protection regime. If the assessment shows that the appropriate safeguard does not provide the required level of protection, then you can include additional measures.

The safeguards are set out below and more detail on the application of each can be found on the ICO's website.

1. A legally binding and enforceable instrument between public authorities or bodies
2. Binding corporate rules (BCRs)
3. Standard contractual clauses (SCCs)
4. An approved code of conduct
5. Certification under an approved certification scheme
6. Contractual clauses authorised by the ICO
7. Administrative arrangements between public authorities or bodies

11.4 Is the restricted transfer covered by an exception?

Where the restricted transfer is not covered by UK adequacy regulations or an appropriate safeguard, then you can only make that transfer if it is covered by one of the 'exceptions' set out in Article 49 of the UK GDPR. These are referred to as true 'exceptions' from the general rule **that you should not make a restricted transfer unless it is covered by UK adequacy regulations or there**

are appropriate safeguards in place.

The exceptions are set out below and more detail on the application of each can be found on the ICO's website.

1. The individual has given explicit consent to the restricted transfer.
2. You have a contract with the individual and the restricted transfer is necessary for you to perform that contract, or you are about to engage in a contract with the individual and the restricted transfer is necessary for you to take steps requested by the individual to enter into that contract.
3. You have (or are about to sign) a contract with an individual which benefits another individual whose data is being transferred. The transfer is necessary for you to either enter into that contract or perform that contract.
4. You need to make the restricted transfer for important reasons of public interest.
5. You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim, or to defend a legal claim.
6. You need to make the restricted transfer to protect the vital interests of an individual. That individual must be physically or legally incapable of giving consent.
7. You are making a restricted transfer from a public register.
8. You are making a one-off restricted transfer and it is in your compelling legitimate interests.

12 Training

It is a legislative and University requirement that individuals subject to this policy must undertake an appropriate level of data protection and information security training reflective of the duties they are performing. Training is an organisational measure which falls under the obligations of the Accountability Principle. For University of Northampton employees, training is mandatory and must be refreshed when it is due.

13 Data Controller

The University of Northampton is the Data Controller for the personal data that this policy applies to.

14 ICO Registration

The University is required to register with the Office of the Information Commissioner in relation to its data protection activities. The registration number can be obtained from Data Protection and Information Governance team and is subject to change in April each year.

15 Data Protection Officer

The University's Data Protection Officer is Miriam Lakin

E: dpo@northampton.ac.uk

16 Data Protection Enquiries

At University of Northampton enquiries relating to privacy rights and data protection matters are managed by the Data Protection and Information Governance team, the team can be contacted at: dpo@northampton.ac.uk.

17 Ownership, approval and review

This policy is owned by the Data Protection Officer. The Data Protection Officer is responsible for ensuring that the policy is reviewed at least every three years, and in response to all relevant changes in law, regulation and good practice. The policy is approved by the University Leadership Team on the recommendation of the Information Security, Governance and Risk Group and following consultation through the Trade Union Liaison Group.

18 Equality Impact Assessment

An Equality Impact Assessment has been completed for this policy.

19 Version Control

Version: 2.0

Date: 01/03/2024

Status: Final

Approved by: University Leadership Team on 19 March 2024

Date of next review: March 2027