THE GENERAL DATA PROTECTION REGULATION (GDPR) POLICY AND PROCEDURE

1 Introduction

This policy supports the legal requirements of the General Data Protection Regulation and the Data Protection Act 2018 which places certain obligations on the University, its staff and those who process data on our behalf. Whilst The University expects its employees and staff to comply with this policy and the requirements of relevant legislation, it does not confer contractual rights or form part of any contract of employment and may be amended by the University or replaced at any time following appropriate consultation and negotiation with recognised trade unions.

Breach of this policy may be addressed via the University's disciplinary and code of conduct policies.

This policy will be reviewed by the Data Protection Officer on a 3 yearly basis. It may however be amended in advance of such date in response to changes in future legislation and/or case law.

2 Ownership

The Human Resources department and Student and Academic Services owns and manages this policy on behalf of The University of Northampton.

3 Organisational Scope

This GDPR policy is a corporate policy and applies to all students, potential students, former, current and potential employees (and workers, as applicable), contractors, visitors and associates of The University of Northampton and any wholly owned subsidiaries unless an alternative policy exists, subject to any qualifying conditions. This policy may form part of any agreements with organisations processing personal data on behalf of the University as if they worked directly for the University.

4 Definitions

4.1 This section includes all necessary definitions of terms used in the policy which are not in every day usage or where there is a need to be precise.

Consent
Consent means offering people genuine choice and control over how you use their data. Consent must be freely and explicitly given to be valid under GDPR

Data Subject
Data subject means "an individual who is the subject of personal data". A data subject must be a living individual.

Information Commissioner's Office (ICO)
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforce the law in regard to information compliance legislation.

Lawful Processing for Legitimate Interests
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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 a 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

Personal data breach
Personal information data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. We are legally obliged to report breaches that are likely to result in a risk to the rights and freedoms of individuals to the ICO and individuals will have to be notified directly by the University.

Processing of Personal Data
Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.

Records Disposal
The University should retain records for only as long as they are needed and then, when they are no longer needed, destroy them in an appropriate manner or dispose of them in some other way, e.g. by transfer to an archives service.

Retention period
The periods of time, varying from a few months to permanency, during which a record has to be maintained by the University. This is usually determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention.

Retention schedule
A retention schedule is a list of records for which pre-determined destruction dates have been established. In the case of the University of Northampton, the retention schedule is combined with the file plan/classification scheme into a single document. This is used as the basis for how long the University should be keeping all data including personal information.

University community
For the purposes of this Policy this includes staff, students, contractors, governors and others with a direct impact on or responsibility to the University

5 Policy Statement

5.1 The University as an institution, and individual members of the University community are expected to abide by the laws in force in this area. All University staff and contractors as well as students processing data on behalf of the University are responsible for any breaches of such legislation and any such breaches may result in disciplinary action, fines or in extreme cases custodial sentences.

6 Key Principles

6.1 The University of Northampton is strongly committed to complying with its legal obligations regarding protecting the personal data and privacy of individuals.

6.2 This Policy and procedure sets out the minimum requirements for data processing by the University so as to protect the rights of data subjects.

6.3 The University needs to keep and process certain information about its employees, students and others to allow it to comply with legal obligations, and to operate in an effective and efficient manner.

6.4 To comply with the existing Data Protection Act requirements and the General Data Protection Regulation, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, University staff, students and contractors must comply with the Principles and protections set out in the Data Protection Act currently in force, GDPR 2018 and reiterated in the University GDPR Policy.

6.5 The University must only retain personal data in line with the guidance set out in the University Retention Schedule. This document provides advice as to retention periods suitable for types of records prior to any disposal decisions being made.

6.6 All processing of personal data under the GDPR needs to have a legal basis, and the University must be able to demonstrate, to the ICO or to the individual, this basis using logged documentation.

6.7 It is important to determine the legal basis for processing as under the GDPR this has an influence on an individual's rights. For example, consent provides individuals with stronger rights such as having data deleted.

6.8 Processing Conditions

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- 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

- Processing is necessary for the purposes of the legitimate interests of the University or the legitimate interests of a third party.

6.9 The GDPR introduces a duty on the University of Northampton to report serious data breaches to the Information Commissioner's Office, and often to the individuals affected. A notifiable breach has to be reported to the ICO within 72 hours of the University becoming aware of it as well as, when appropriate, notification to the data subject within the same tight timescale.

6.10 Fines have increased and the maximum fines can be up to 20 million Euros or 4% Global Turnover for a breach, depending on the severity, scale or impact of the breach. For example the loss of hundreds of minor pieces of personal information might incur a smaller fine than a case where the University loses the sensitive personal health information of one individual.

6.11 Failure to report a breach can also result in fines for the University and potentially for the individual who has committed the breach. The University requires all incidents and breaches to be reported so we can assess and reduce the risks and where possible prevent incidents from becoming serious breaches. Failure to report a breach may result in disciplinary action. A breach by an individual may result in additional training being provided. Continuing or serious breaches of personal data may result in disciplinary action being taken by the University.

6.12 All employees must undertake the GDPR e-learning which is part of the University's mandatory training programme Persistent failure to undertake this e-learning may result in disciplinary action.

6.13 Unauthorised audio recording of conversations is prohibited. Anyone in breach of this may be subject to disciplinary action.

7 Procedure

Data Held and Processed by the University

7.1 The University will use and otherwise process records of personal information relating to data subjects relevant to the effective functions and operation of its role as a Higher Education Institution and employer.

7.2 Where required, The University will obtain freely given consent for all types of personal data processing except that specifically exempted by the Regulation.

7.3 The use of the information and retention of the personal data will be specifically defined within the University central personal data processing log.

7.4 All staff, students and other data subjects about whom personal information is held may have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Some of these rights may be restricted depending on the lawful basis the University is relying on for the processing can also affect which rights are available to individuals. The ICO provides the following examples:

	Right to erasure	**Right to portability**	**Right to object**
Consent	✓	✓	**X** but right to withdraw consent
Contract	✓	✓	**X**
Legal obligation	**X**	**X**	**X**
Vital interests	✓	**X**	**X**
Legitimate interests	✓	**X**	✓

The new rights are explained further in Appendix A

7.5 This adds to the existing rights previously in place for data subjects which include a person's right to know:

- what information the University holds and processes about them
- why the information is held and processed
- details of whom the information might be shared with
- know how to gain access to such information
- know that it is up to date
- know what the University is doing to comply with its obligations under the Data Protection Act or other relevant legislation

8. Responsibilities of Staff in Relation to their own Data

8.1 All staff are responsible for:

Checking that any personal data that they provide to the University is accurate and up to date (they will be asked by the University to check this periodically). Informing the University of any changes or errors in the information held.

9. Responsibilities of Students in Relation to their own Data

9.1 Students will, at the time of registration, be required to agree to the use of personal data for university administrative purposes, which will be clearly specified. This will notify students of the uses we are making of their personal data and will form a contract between the University and the student.

9.2 Students must assist the University in ensuring the accuracy of the personal data as provided to the University and that the information is up to date. Any changes of address, etc. are to be notified to the relevant administrative office. They will be asked to check the accuracy of the information at enrolment each year. Changes made by the student to the accuracy of the data the University holds on them will not alter the basis of the contract between the University and them.

10. Basic responsibilities on staff for Data Security of Third Party Personal data

10.1 The University has a legal requirement to ensure that data is held securely and this includes the provision that access and disclosure of personal data should be restricted to those who have a legitimate, authorised purpose.

10.2 Staff have a responsibility for using and otherwise processing personal data in compliance with this Policy and more specifically operating under the terms of the relevant Data Protection legislation.

10.3 Therefore, 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 should be locked or password protected when not in use
- No personal information should be removed from the University buildings unless it is via a secured electronic means
- Staff processing personal data for research purposes (for example, use of questionnaires) should include a Data Protection Notice informing the data subject of details such as why the data is being collected and how long it will be retained for. If in doubt please contact the Records Management Office for advice.

11. Responsibilities on students for Data Security of Third Party Personal data

11.1 Students may need to process personal information for project or research purposes such as surveys, etc. Such documents should include a Privacy Notice (Data Protection Notice) informing the data subject of details such as why the data is being collected and how long it will be retained for. If students are processing personal data then they must obtain appropriate approval from the relevant authority and any such collection of personal data should need the approval of the Research Ethics Committee.

12. Right of Access to Information

12.1 The ICO provides information regarding valid requests for a data subject to access their personal data (A Subject Access Request).

- it should be made in writing.
- A request sent by email or fax (and potentially via social media) is as valid as one sent in hard copy.
- You do not need to respond to a request made verbally… it is good practice to at least explain to the individual how to make a valid request, rather than ignoring them.
- If a disabled person finds it impossible or unreasonably difficult to make a subject access request in writing, you may have to make a reasonable

adjustment for them under the Equality Act 2010. This could include treating a verbal request for information as though it were a valid subject access request.

- If a request does not mention the Act specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own personal data.
- A request is valid even if the individual has not sent it directly to the person who normally deals with such requests – so it is important to ensure that you and your colleagues can recognise a subject access request and treat it appropriately.

12.2 All data subjects have the right to apply for access to any personal data that is being kept by the University about them either on computer or in certain other files. Any student who wishes to exercise this right should make a written request to the Director of Student & Academic Services or to the University Data Protection Officer. Staff should make a written request to the Director of Human Resources or to the University Data Protection Officer. The University cannot charge any fee or disbursement for such a service and must make all efforts to provide the personal data in a format defined by the requester.

12.3 All requesters will be asked to include proof of identity and no response will be sent until such proofs have been provided. The University will ensure that requests for information are responded to within the statutory month period unless additional information has been requested by the university to help identify the requested data. In such cases, the reason for delay will be explained in writing by the Data Protection Officer to the person making the request.

12.4 Third party information will normally be redacted in lines with the rights of such third parties.

13. Publication of University Information

13.1 Information that is already in the public domain, and accepted by the data subject as being so, is less likely to be covered by the legislation. For example, externally circulated publications and web pages. However, the GDPR does provide, in certain circumstances, for a data subject to have the right of erasure of personal data. This is a complex area and any member of staff receiving such a request should contact the University Data Protection Officer. Any individual who believes that they have good reasons to have their information excluded from any such publications or released data should inform the relevant Dean or Head of Department who will coordinate with the Data Protection Officer.

14 Personal Data Breach

14.1 All personal data breaches should be reported to the local Data Protection Co-ordinator (DPC) and relevant line management who will make a judgement on the severity of the breach.

14.2 Breaches involving large losses or misuses of personal data or any involving 'sensitive' personal data will be reported by the DPC to the Data Protection Officer to investigate more fully. To help Data Protection Co-Ordinators to identify the seriousness of a breach please refer to Appendix B and Appendix C.

14.3 Additionally in the case of an electronic data breach as a result of hacking or wide-scale misuse of the University computer systems, the Director of IT Services should also be notified.

14.4 In the event of a theft of data or a device containing data when away from the University, the police should also be notified of the theft by the line manager.

15 Actions to be taken in Response to a Personal Data Breach

15.1 As soon as a breach has been detected or is suspected the following steps should be taken:

15.1.1 An immediate attempt should be made by the line manager or Co-Ordinator to recover any personal data lost or misplaced.

15.1.2 Liaise with those involved with the Breach to prevent the further worsening of any breach.

15.1.3 Consideration should be given as to whether to notify those affected by any such Breach. The University is strongly in favour of notifying those affected but in any event those who may suffer damage (including reputational damage) or loss should always be informed.

15.1.4 Steps should be taken to review processes and procedures to reduce the risk of further breaches happening again.

15.1.5 Systems and procedures will be reviewed by the Data Protection Co-Ordinator 3 months after the breach to make sure processes have been made more robust.

15.1.6 Where relevant, those affected should be informed of the steps that have been taken to recover their personal data and reviews that have started to prevent issues happening in the future.

15.1.7 Those responsible for major breaches or repeat minor breaches will be required to undertake further remedial Data Protection training and may be reported by the DPC or DPO to their line manager.

15.1.8 In the case of serious Breaches, deliberate breaches or repeated breaches after training, the individual will be subject to disciplinary action.

15.1.9 In the case of serious breaches the University Data Protection Officer will be legally obliged to report such a breach to the Information Commissioner's Officer. This may result in fines for the University and for those committing major breaches.

15.1.10 Where the ICO has been notified of a breach the Press Office, the Chief Operating Officer and Vice Chancellor will be informed.

15.1.11 If appropriate in the case of deliberate or malicious breaching of personal data the COO may where appropriate inform the police and University insurance suppliers.

15.1.12 The DPC's will keep a record of all breaches, what action has been taken and by whom.

15.1.13 The Data Protection Officer will retain records for all serious breaches.

14. Associated Documents

14.1 External associated documents:

The General Data Protection Regulation 2018

Data Protection Act 2018

Privacy and Electronic Communications Regulation

Information Commissioner's Office Overview of the General Data Protection Regulation (GDPR)

Information Commissioner's Office Privacy Notices, Transparency and Control – a code of practice on communicating privacy information to individuals

Information Commissioner's guide to data protection

Information Commissioner's Office GDPR Consent Guidance (Currently in consultation)

Information Commissioner's Office Guide to Privacy and Electronic Communications Regulation

Freedom of Information Act 2000

15. Internal associated documents

Guidance on the Storage, Transmission and Use of Personal and Confidential Information Outside of Computing Systems Provided by the University

Disposal of Records Process (new process in development)

Records Retention Schedule (As of March 2018 this is under review)

16. Equality Analysis

There is no adverse equality impact within this policy. All responses to breaches of rights will be dealt with in accordance with this Policy, Procedure and relevant Appendices irrespective of an individual's specific characteristics.

17. Version Control

Version Control		**Approval record**	
Author:	Phil Oakman	Approval:	TU Liaison – 20/3/18 UMT – 27/3/18 Board – 18/4/18
Date written:	June 2017	Updates:	January 2018
Current status:	Live		
Record of Amendments			
Date	Details of Change		Approval
28th June 2017	Data Protection Policy amended to take account of the General Data Protection Regulation		
January 2018	More detail provided in line with ICO guidance		April 2018

Appendix A - New Rights (Based on Information Sourced from the Information Commissioners Office website)[1]

Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances, which are:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent (if consent has provided the justification for processing).
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- This right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.
- There are some specific circumstances where the right to erasure does not apply and the University may refuse to deal with a request. We may refuse to comply with a request for erasure where the personal data is processed for the following reasons:
- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ Accessed 13/02/2018

Right to Data Portability

- The right to data portability 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 hindrance to usability.
- However the right to data portability only applies:
- to personal data an individual has provided to the University;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Right to Object

Individuals have the right to object to:

- processing based on legitimate interests (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.
- Individuals must have an objection on "grounds relating to his or her particular situation". The University will have to stop processing the personal data unless:
- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.
- We must inform individuals of their right to object "at the point of first communication" and in relevant privacy notices.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Specific Right to Object to Direct Marketing Purposes

The University must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

Dealing with such an objection to processing for direct marketing must happen promptly and free of charge.

The University must inform individuals of their right to object “at the point of first communication” and in relevant privacy notices. This must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information”.

Specifics Regarding Right to Object about Research Purposes?

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

There will, in certain circumstances an exemption under Article 89 that will allow the continued processing even after receiving an objection

Appendix B Examples Of Incidents Which Should Be Investigated

This will not be a complete list but is designed to provide advice as to potential breaches that may occur.

- Sending emails or correspondence containing personal data to the wrong recipient;

- Sending non-essential personal data to otherwise valid recipients (for example including a string containing health details to all recipients when only one has rights to see it);

- Personal data received in error;

- Failure to secure access to University devices, including incorrect allocation of permissions or sharing passwords, which result in unauthorised access to personal data. Staff in business areas have responsibility for access controls but IT and the Records Management Office can provide advice on how to improve security arrangements;

- Misuse of University computer systems to access personal details where there is no business purpose to do so

- Loss or theft of any university-owned data storage device regardless of the data it contains e.g., laptop, PC, USB/pen drive, iPad or other tablet, removable hard drive, smart phone or other portable devices; or

- Accidental publication of personal data on a website;

- Loss or theft of papers containing personal data;

- Theft of any privately owned devices should also be reported if they have been used to process personal data related to university staff or students.

APPENDIX C Guidance to Data Protection Co-Ordinators on Assessing Breaches.

This is intended as a guide only and not all specific circumstances may be included in the table – If in doubt please contact the Data Protection Officer for additional advice and support.

No. of individuals whose data has been disclosed or otherwise put at risk	Very Minor Incident	Minor Incident	Serious Incident	Major incident
0-100 with one or more of the following characteristics : • No sensitive personal data • Information already accessible or in public domain • Low level of harm to individuals				
101 plus with one or more of the following characteristics : • No sensitive personal data involved • Information already accessible or in public domain • Low level of harm to individuals				
0-100 with one of the following characteristics : • One or more previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information				

101 plus with one or more of the following characteristics : • Several previous similar incidents in last 12 months • Failure to implement, enforce or follow technical safeguards to protect information				
0-100 with one of the following characteristics: • Detailed information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				
0-100 with more than one of the following characteristics: • Detailed				

information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				
101-plus with one or more of the following characteristics: • Detailed information at risk e.g. clinical care case notes, social care notes • High risk confidential information • Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual • Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment • Individuals likely to have been placed at risk of incurred physical harm				

Appendix D Points for Investigating Staff to Consider

- What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
- How did the breach occur?
- What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)
- How many individuals or records are involved?
- If the breach involved personal data, who are the individuals? (Students, staff, research participants etc)?
- What has happened to the data?
- Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
- Were there any protections in place? (e.g. Encryption)
- What are the potential adverse consequences for individuals or the University? How serious or substantial are they and how likely are they to occur?
- What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
- What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

APPENDIX E: Breach Log Template

Completed forms to be retained by DPC unless it represents a major breach in which case it should be forwarded on to the DPO for further action.

Questions	Answers
When did this Breach occur? When was it reported?	
What are the personal data affected?	
How many people will have been affected?	
Where are the data now and how many people with no rights to access it have seen it?	
What has been done to recover the data?	
What policies or procedures have been put in place or amended to stop a recurrence of this Breach?	
What training/ awareness raising measures have been taken in the light of this Breach?	
Has this happened before?	
Is disciplinary action recommended?	