Privacy and Personal Data Protection Policy

Version:	**1.0**
Dated:	**02 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
V 1.0	02/05/2018	R. Platt	Amendment to Section 2 and approval for publication
V 0.5	27/04/2018	R. Platt & R. Cockram	Review of suggestions and comments from contributors. Document formatting.
V 0.4	26/04/2018	R. Cockram	Incorporating comments and clarifications from Chris Lindsay.
V 0.3	26/04/2018	D. Bristow	Spelling, Grammar and comments.
V 0.2	26/04/2018	R. Cockram	Spelling, Grammar and comments.
V 0.1	24/04/2018	R. Platt	Initial Draft.

Approval

Approval Board	Date of Approval
Information Governance & Security Steering Group	02/05/2018

Contents

List of Tables

1 Introduction

1.1. The University of Exeter is committed to protecting the fundamental rights and freedoms of individuals including their right to privacy with respect to the processing of their personal data. This policy is a statement of the key measures which the University has adopted to ensure good practice and compliance with the requirements of relevant data protection legislation. This policy is supported by a range of guidance materials and should be read in conjunction with other relevant University Policies and Procedures including those listed in sections 3 and 4.

1.2. Data protection legislation applies to personal data held in any format (paper, electronic, microfiche, tape etc.). The University recognises that its priority is to protect privacy and to avoid causing harm to individuals. This means ensuring that high quality personal information processed securely and appropriately. The legislation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are considered. In addition to being open and transparent, the University will seek to give individuals as much choice as is possible over what data is processed and how.

1.3. In its everyday business operations the University of Exeter makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective Students and Alumni,
- Current, past and prospective Employees,
- Users of its Websites,
- Users of its Services,
- Research Participants, and
- Other stakeholders

1.4. In collecting and using these data, the University is subject to a variety of legislation controlling how such activities may be carried out as well as the safeguards which must be put in place to protect it. The purpose of this policy is to set out the relevant legislation and to describe the steps the University is taking to ensure the institution is compliant.

1.5. This policy applies to all staff working for, or on behalf of, the University and includes direct employees, employees of other organisations working for or in association with the University of Exeter, associates and contractors or other third parties with legitimate access to University data or systems. In addition, students, volunteers and data processors are expected to comply when working on behalf of the University.

2 Responsibilities

The University of Exeter is the 'data controller' and the Council of the University, as the governing body, is ultimately responsible for compliance with current data protection legislation. The University will take the appropriate measures to ensure compliance and to protect data subject's rights under the legislation.

2.1 Information Users

All members of the University are responsible for complying with all relevant data protection legislation and this policy.

All members of the University must also ensure that any personal data they supply to the University are accurate and up-to-date.

2.2 Senior Information Officers (SIO) – Colleges and Services

Director of College Operations and Directors of Professional Services have the responsibility of overseeing compliance and developing good data protection practice within their designated areas.

2.3 Managers and Supervisory roles

All employees in managerial or supervisory roles have the responsibility of overseeing compliance and developing good data protection practice within their designated areas.

Managers should ensure that staff have completed the mandatory Information Governance online training.

2.4 Information Asset Owners (IAO)

IAOs are responsible for ensuring their information assets are identified, included on the University Information Asset Register and compliant with this policy and relevant data protection legislation.

2.5 Data Protection Officer (Information Governance Manager)

In accordance with the GDPR the University has appointed a Data Protection Officer (the Information Governance Manager) to carry out the DPO role as defined in the legislation. The DPO is responsible for dealing with day-to-day data protection matters, providing training and for developing and encouraging good information handling practice amongst all members of the University.

3 Privacy and Personal Data Protection Policy

3.1 The General Data Protection Regulation

The General Data Protection Regulation (‘GDPR') is one of the most significant pieces of legislation affecting the way that the University carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is the University’s policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

3.2 Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

> *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;*

‘processing’ means*:*

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, University, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

‘controller’ means*:*

> *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

3.3 Principles Relating to Processing of Personal Data

There are several fundamental principles upon which the GDPR is based.

These are as follows:

1. Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

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 erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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 or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The University will ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

3.4 Rights of the Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within the University that allow the required action to be taken within the timescales stated in the GDPR.

For more information see the *Data Subject Request Procedures*

These timescales are shown in Table 1.

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	One month
The right to restrict processing	Without undue delay & within one month
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

Table 1 - Timescales for data subject requests

3.5 Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is the University's policy to identify the appropriate basis for processing and to document it in the University's Information Asset Register, in accordance with the Regulation. The options are described in brief in the following sections.

3.5.1 Performance of a Contract

The processing is necessary for a contract the University has with the individual, or because they have asked us to take specific steps before entering into a contract. This will be appropriate where the contract cannot be completed without the personal data in question e.g. student contracts and employment contracts.

3.5.2 Legal Obligation

The personal data is required to be collected and processed in order to comply with the law (not including contractual obligations). This may be the case for some data related to employment and taxation, and for example the University is required by law to provide data to HESA in relation to both staff and students.

3.5.3 Vital Interests of the Data Subject

In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, that is to protect someone's life, then this may be used as the lawful basis of the processing. The University will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used when a student/staff member has an accident and we are required to share their personal data with the emergency services.

3.5.4 Task Carried Out in the Public Interest

The processing is necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law. Where the University needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested, this includes processing personal data for teaching and research purposes. The assessment of the public interest or official duty should be documented and made available as evidence where required.

3.5.5 Legitimate Interests

If the processing of specific personal data is in the legitimate interests of the University and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

3.5.6 Consent

Consent from the data subject for processing of their personal data is only required where none of the other lawful conditions of processing applies and must be freely given. When consent is required the University will ensure that it is compliant with GDPR legislation and involves a clear affirmative action (opt-in). It must be kept separate from other terms and conditions, specific and granular, clear and concise. Clear records must be kept to demonstrate consent and data subjects should be able to withdraw their consent in a manner as simple a method by which the consent was originally given.

In case of children below the age of 13 parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

3.6 Privacy by Design

The University has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of Data Protection Impact Assessments (DPIA)

The Data Protection Impact Assessment will include:

- Consideration of how personal data will be processed and for what purposes.
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to individuals in processing the personal data.
- What controls are necessary to address the identified risks and demonstrate compliance with legislation.

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

The University requires all new or significantly changed systems, or new information assets must be assessed for a DPIA, and where appropriate a light touch or full DPIA will be carried out.

For more information see the *Data Protection Impact Assessment Policy.*

3.7 Contracts Involving the Processing of Personal Data

The University will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

3.8 International Transfers of Personal Data

Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

3.9 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under the GDPR for the University. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Information Governance Manager is the appointed University of Exeter DPO and, for data protection matters, reports directly to VCEG. The University Registrar & Secretary, who acts as the Senior Information Risk Owner (SIRO) is the point of contact for VCEG. In circumstances where it is more appropriate, concerns may be raised directly with the Vice-Chancellor, Chair of Audit Committee or Chair of the Council of the University.

The DPO's role includes monitoring internal compliance, advising on data protection obligations, providing advice regarding Data Protection Impact Assessments and acting as a contact point for data subjects and the Information Commissioners Office (ICO).

The University must ensure the DPO is closely involved in all data protection matters in a timely manner, including DPIAs. The DPO must be given adequate resources and appropriate access to personal data, processing activities and other services to enable them to carry out the DPO role as defined in the GDPR.

3.10 Breach Notification

It is the university's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours.

For more information see the *Data Breach Policy.*

Under the GDPR the relevant Data Protection Authority has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

3.11 Addressing Compliance to the GDPR

The following actions are undertaken to ensure that the University complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous.
- A Data Protection Officer is appointed with specific responsibility for data protection in the University.
- All staff involved in handling personal data understand their responsibilities for following good data protection practice.
- Training in data protection has been provided to all staff.
- Rules regarding consent are followed.

- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
- Regular reviews of procedures involving personal data are carried out.
- Privacy by design (DPIAs) is adopted for all new or changed systems and processes.
- The following documentation of processing activities is recorded:
    - University name and relevant details,
    - Purposes of the personal data processing,
    - Categories of individuals and personal data processed,
    - Categories of personal data recipients,
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place,
    - Personal data retention schedules and
    - Relevant technical and organisational controls in place.

These actions are reviewed on a regular basis as part of the management process concerned with data protection.

4 Further Information and related policies

4.1 Related Policies and Guidance

This policy should be read in line with associated standards, policies and arrangements including:

1.1 Associated policies

- Information Security Policy
- *Data Breach Policy*
- Records Management Policy
- Records Retention Schedules

1.2 University Guidance and Standards

- Information Governance Web Pages
- Data Breach Reporting Web Page
- *Data Protection Impact Assessment Process*
- *Legitimate Interest Assessment Procedure*
- *GDPR Roles and Responsibilities*

1.3 External Resources

- ICO Guide to the GDPR
- General Data Protection Regulation

For further information contact the University's Data Protection Officer/Information Governance Manager.