

# Data Protection Policy

Data Protection Officer  
December 2021



UNIVERSITY OF  
**WINCHESTER**

<b>Document Title</b>	Data Protection Policy
<b>Document Author and Department:</b>	Stephen Dowell, University Data Protection Officer and Melanie Short, Information Compliance Officer, SMG
<b>Responsible person and Department:</b>	Stephen Dowell, University Data Protection Officer, SMG
<b>Approving Body:</b>	University Management Group
<b>Review Date:</b>	November 2022
<b>Date latest edition comes into force:</b>	Immediately
<b>Edition (Date of Approval)</b>	20 December 2021
<b>Indicate whether the document is for public access or internal access only</b> <b>Indicate whether the document applies to collaborative provision?</b>	<b>Public Access</b> <del>Internal Access Only</del> <b>Applies to Collaborative Provision</b>
<b>Summary:</b>	
<p>The Data Protection Policy ensures the University's compliance with the Data Protection Act 2018, UK and EU GDPR.</p> <p>This version updates the Policy which was approved by Planning and Resources Committee in October 2020.</p>	

## Contents

1	Introduction .....	4
2	The Data Protection Principles.....	4
3	Data Subject Rights.....	4
4	Compliance with the Policy .....	5
5	Responsibilities of All Data Users .....	6
5.1.	Lawful processing.....	6
5.2.	Retention of personal data.....	6
5.3.	New or additional processing.....	6
5.4.	Research .....	7
5.5.	Data Security .....	7
5.6.	Data Breaches .....	7
6.	Responsibilities of Applicants and Students as Data Subjects.....	8
7.	Responsibilities of Employees as Data Subjects.....	8
8.	Closed Circuit Television.....	8
9.	Data-Sharing.....	8
9.1.	Internal Data Sharing .....	9
9.2.	Sharing of Staff and Student Data with Third Parties, including Parents and Guardians. ....	9
9.3.	External Data Sharing to and from the University .....	9
10.	Transfers of Personal Data Outside the UK .....	9
11.	Further Information .....	10

## 1 Introduction

The University of Winchester treats very seriously both the personal data and the sensitive personal data it processes on behalf of its students and staff members, and the wide range of other people with whom it works and has contact with. The information and guidelines contained within this policy and its accompanying guidance apply to the whole University community of staff and students.

Under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR), the University is classed as a data controller. The University is also required to comply with the EU General Data Protection Regulation (EU GDPR) when processing the personal data of citizens of the European Union. The principles and rights of individuals contained within the EU GDPR are the same as the UK GDPR. For the purposes of this policy the term 'GDPR' will apply to both the EU GDPR and the UK GDPR. Like all educational establishments, the University holds and processes personal data, about its employees, students, applicants, alumni and other individuals for a variety of purposes. These purposes include the administration of the admissions process, the effective provision of academic and welfare services, recording academic progress, operating payroll, and to enable correspondence and communications. There may also be occasions where the University is required to process sensitive personal data. Definitions of 'personal data' and 'sensitive personal data' (also known as special categories of personal data in the GDPR) can be found [here](#)

To comply with the DPA 2018 and GDPR, this personal data must be processed in line with the GDPR principles.

## 2 The Data Protection Principles

The GDPR sets out seven key principles:

- a) Lawfulness, fairness and transparency
- b) Purpose limitation
- c) Data minimisation
- d) Accuracy
- e) Storage limitation
- f) Integrity and confidentiality (security)
- g) Accountability

These principles lie at the heart of the University's approach to processing personal data.

## 3 Data Subject Rights

GDPR provides the following rights for individuals:

- a) **The right to be informed**

You have the right to be informed about the collection and use of your personal data.

The University has produced a standard privacy notice, which sets out how the University processes personal data, and this can be accessed [here](#).

The University also uses shorter and more tailored privacy notices to make them more easily accessible to the respective data subjects.

b) **The right of access**

You have the right to ask the University for copies of your personal information; this is also known as a Subject Access Request.

c) **The right to rectification**

You have the right to ask the University to rectify information you believe is inaccurate. You also have the right to ask us to complete information you think is incomplete.

d) **The right to erasure**

You have the right to ask the University to erase your personal information in certain circumstances.

e) **The right to restrict processing**

You have the right to ask the University to restrict the processing of your personal data in certain circumstances.

f) **The right to data portability**

You have the right to ask that the University transfers the information you provided to another organization, or to you, in certain circumstances.

g) **The right to object**

You have the right to object to the processing of your personal data in certain circumstances.

h) **Rights in relation to automated decision making and profiling.**

You have the right to be informed about automated individual decision-making and profiling.

None of these rights are absolute and further information about the rights, including the circumstances where they may apply is available from the Information Commissioner's Office (ICO) [here](#).

To exercise your rights and/or for further advice and guidance, please contact the Data Protection Officer or the Information Compliance Officer.

#### **4 Compliance with the Policy**

Compliance with the DPA 2018 and GDPR is the responsibility of all employees and students at the University.

Any deliberate breach of the Policy may lead to access to university facilities being withdrawn, disciplinary action being taken, or even to criminal prosecution.

Any questions or concerns about the interpretation or operation of this policy should be referred to the University's Data Protection Officer.

## **5 Responsibilities of All Data Users**

### **5.1. Lawful processing**

All personal data needs to be processed in line with the lawful bases set out in the GDPR. Further information is available from <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>.

When special category data is processed, it is necessary to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 ([UK GDPR](#)).

### **5.2. Retention of personal data**

The GDPR sets out the principle that personal data shall be 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 when the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

This is subject to implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals.

Further information about how the University stores and retains personal data can be found in the Records Management Policy.

### **5.3. New or additional processing**

Employees of the University must not do any of the following, without the proper authorisation and approval from their head of department:

- a) Develop, purchase or subscribe to a new computer system/platform for processing personal data
- b) Use an existing computer system to process personal data for a new purpose
- c) Create a new electronic or paper filing system, including spreadsheets' containing personal data
- d) Use an existing electronic or paper filing system, including spreadsheets' containing personal data for a new purpose

All new software and systems **must** be approved and procured through IT Services, who will check for technical, security and data protection compliance.

In certain circumstances (for example, the introduction of new technologies, systems, software, or a new process) a Data Protection Impact Assessment (DPIA) may be required.

ICO guidance on Data Protection Impact Assessments can be found [here](#).

Please contact the Data Protection Officer for further guidance.

#### **5.4. Research**

The DPA 2018 and GDPR include specific exemptions for the processing of personal data that is necessary for archiving purposes, scientific or historical research purposes or statistical purposes. For further information, see paragraph 620 of the [Explanatory Notes](#) to the DPA 2018.

#### **5.5. Data Security**

A key principle of the GDPR is that personal data must be processed securely by means of 'appropriate technical and organisational measures'.

All employees of the University are responsible for ensuring that:

- a) Any personal data which they hold, or process is kept securely
- b) Personal data is not disclosed orally or in writing or otherwise to any unauthorised third parties, and that every reasonable effort is made to see that personal data is not disclosed accidentally (see also 9.2)
- c) All third-party requests for access to personal data, including those from the police, are directed to the University Data Protection Officer.
- d) Unauthorised disclosure may be a disciplinary matter. If you are in any doubt consult the Data Protection Officer.

Further guidance is available on the [University intranet](#) and on the ICO website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/>.

#### **5.6. Data Breaches**

Any unauthorized or accidental disclosure of personal data should be considered a data breach. It is the responsibility of every student and member of staff to report data breaches, actual or potential, whether they are directly involved in the breach or not. Breaches must be reported to the Data Protection Officer and the Information Compliance Officer as soon as possible, detailing what remedial action may have already been taken. They will work together with the aim of minimizing the effects of the breach and users must co-operate promptly to requests for further information relation to the scope of the incident. Failure to follow this guidance may result in disciplinary action.

All data breaches will be logged internally by the University, and this information may be used to determine which departments require retraining.

Data Protection legislation gives the University a duty to report certain types of personal data breach to the Information Commissioner's Office as the Supervisory Authority within 72 hours of becoming aware of the breach, where feasible., It is therefore essential that all breaches are reported immediately.

## **6. Responsibilities of Applicants and Students as Data Subjects**

Applicants and students must ensure that any personal data supplied to the University is accurate and up to date. They must ensure that any changes of address or other personal details are notified to UCAS in the case of applicants or in the case of students to update their personal details via 'My Record'.

Students using University computing facilities are required to comply with the data protection provisions of the University IT Acceptable Use policy.

Students involved in organizing clubs and societies are also obliged to comply with the DPA 2018 and GDPR.

### **6.1. Student Union**

Please be aware that for the purposes of data protection and this policy, the Student Union is a separate organisation from The University of Winchester. This means that care must be taken when sharing any personal data with the Student Union, but it can be done where the University has a 'lawful basis' (a legal ground) to do so. The Student Union and the University of Winchester have a data sharing agreement to make such data sharing between the two clearer and easier to understand. Students involved in organizing clubs and societies through the Students Union are still obliged to comply with the DPA 2018 and GDPR.

## **7. Responsibilities of Employees as Data Subjects**

All employees must ensure that the personal data they supply to the University is accurate and up-to-date, and that the University is informed of any errors in, or changes to, information which they have provided, e.g. changes of address or marital status. Some of these changes can be made through iHR accounts.

## **8. Closed Circuit Television**

The University uses Closed-Circuit Television and Body Worn Video equipment as part of its security system. This is done in accordance with the [CCTV Data Protection Code of Practice](#), issued by the Information Commissioner's Office.

## **9. Data-Sharing**

When considering a new data sharing process, you must assess your overall compliance with the data protection legislation. This may include the need for a Data Protection Impact Assessment (DPIA) or the need for a data sharing agreement between the University and the external party. These should be reviewed and signed off by the Data Protection Officer or Information Compliance Officer.

The ICO has produced a data sharing code of practice which can be found [here](#).

The code is mainly aimed at organisations that are controllers sharing personal data. It is aimed at data protection officers (DPOs) and other individuals within organisations who are



responsible for data sharing matters. The code contains practical guidance on how to share data fairly and lawfully, and how to meet your accountability obligations.

It does not impose any additional barriers to data sharing but it will help you comply with your legal obligations under the GDPR and the DPA 2018.

### **9.1. Internal Data Sharing**

Organisations such as the University are able to share personal data within themselves as long as there is a legitimate business reason ( i.e. a 'need' to do so).

More technically, a sharing of personal data within any organisation would still be a processing of that 'personal data', and so would still be subject to the GDPR (General Data Protection Regulation) and the seven GDPR 'principles' (see section 2)

### **9.2. Sharing of Staff and Student Data with Third Parties, including Parents and Guardians.**

Data protection laws protect an individual's right to privacy with regards to their personal data and establish a set of principles and conditions about its use and disclosure which the University must comply with.

The University of Winchester will not disclose personal data about its staff and students to any third party, including parents and guardians. This will include confirming that an individual is a student or an employee; to do so could infringe privacy and may, in extreme circumstances, place an individual in danger. Disclosure must only happen with the informed written consent from the member of staff or student for their information to be released to named individuals. If you are in any doubt of how to handle a third-party request of this nature, please refer to the guidance available [here](#) or contact the Data Protection Officer.

### **9.3. External Data Sharing to and from the University**

Sharing personal data externally should only be done in compliance with the data protection principles and there must be a clear and lawful reason for doing so. Data sharing can take place in a routine, scheduled way or on a one-off basis. When needed it can be shared in urgent or emergency situations.

## **10. Transfers of Personal Data Outside the UK**

The ICO's GDPR [guidance](#) on these transfers is as follows:

*"The UK GDPR primarily applies to controllers and processors located in the United Kingdom with some exceptions. Individuals risk losing the protection of the UK GDPR if their personal data is transferred outside of the UK.*

*On that basis, the UK GDPR restricts transfers of personal data outside the UK, or the protection of the UK GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies.*

*A transfer of personal data outside the protection of the UK GDPR (which we refer to as a 'restricted transfer'), most often involves a transfer from the UK to another country".*

Transfers of personal data to countries that are covered by UK "adequacy regulations" are permitted. These are countries that have been assessed as providing 'adequate' protection for individual rights and freedoms for their personal data. Under provisional arrangements all countries within the European Economic Area (EEA) are considered to be 'adequate', therefore transfers of personal data to these countries are permitted.

Other countries that are covered by the adequacy regulations are Andorra, Argentina, Gibraltar, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

It is essential that all new additional software and systems go through the compliance checks outlined in paragraph 5.5 of this policy. This is done to ensure that transfers out of the UK do not take place if there are no necessary additional safeguards or adequacy arrangements.

If you need any further advice and guidance about transfers of personal data outside the UK, please contact the Data Protection Officer or the Information Compliance Officer.

## **11. Further Information**

Any queries relating to this policy and its implementation should be raised first with the Data Protection Officer for the University. His contact details are [stephen.dowell@winchester.ac.uk](mailto:stephen.dowell@winchester.ac.uk) , 01962 827217

If a data subject is not satisfied with the way the University has processed their personal data, there is a right to lodge a complaint with the Information Commissioner's Office, who can be contacted in various ways as listed at:

<https://ico.org.uk/global/contact-us/>

### **Related University Policies:**

[ICT Acceptable Use Policy](#)

[Information Security Incident Response Plan](#)

[Records Management Policy](#)

[Website Privacy and Cookie Policy](#)