Data Protection Policy

Director of IT Services
July 2018

UNIVERSITY OF WINCHESTER

Document Title	Data Protection Policy
Document Author and Department:	Sue Mullen, Director of IT Services
Responsible person and Department:	University Data Protection Officer
Approving Body:	Planning and Resources Committee
Review Date:	31 July 2019
Date latest edition comes into force:	Immediately
Edition (Date of Approval)	26 June 2018
Indicate whether the document is for public access or internal access only **Indicate whether the document applies to collaborative provision?**	**Public Access** ~~Internal Access Only~~ **Applies to Collaborative Provision**
Summary:	
The Data Protection Policy ensures the University's compliance with the Data Protection Act	

2018 and GDPR.

This version replaces the previous Policy which was approved in 2011. Minor modification in 2013

Contents

1 Introduction

The University of Winchester is a data controller under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR). The information and guidelines contained within this policy and its accompanying guidance apply to the whole University community, both staff and students.

Like all educational establishments, the University holds and processes information (personal data) about its employees, applicants, students, alumni and other individuals (data subjects) for a variety of purposes such as the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll, and to enable correspondence and communications.

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

Definitions of 'personal data' and 'sensitive personal data' (also known as special categories of personal data in the GDPR) can be found at this link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/.

2 The Data Protection Principles

The GDPR sets out seven key principles:

•Lawfulness, fairness and transparency
•Purpose limitation
•Data minimisation
•Accuracy
•Storage limitation
•Integrity and confidentiality (security)
•Accountability

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

3 Data Subject Rights

The GDPR provides the following rights for individuals:

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.

None of these rights are absolute and further information about the rights, including whether they may apply in particular circumstances, is available from the ICO website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/.

4 Compliance with the policy

Compliance with the DPA 2018 and GDPR is the responsibility of all employees and students of the University. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, access to University facilities being withdrawn, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be referred to the University Data Protection Officer.

4.1 Responsibilities of all data users

4.1.1 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 (GDPR).

4.1.2 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 in order 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.

4.1.3 New or additional processing

No employee of the University may, without the prior authorisation of the University Data
Protection Officer:

- Develop, purchase or subscribe to a new computer system/platform for processing personal data
- Use an existing computer system to process personal data for a new purpose
- Create a new manual filing system containing personal data
- Use an existing manual filing system 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 and security compliance. In certain circumstances (for example, the introduction of new technologies, systems or software) a Data Protection Impact Assessment (DPIA) may be required. For further information see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

Please contact the Data Protection Officer for further guidance.

4.1.4 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:

- Any personal data which they hold or process is kept securely
- Personal data is not disclosed orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort is made to see that personal data is not disclosed accidentally
- All third party requests for access to personal data, including those from the police, are directed to the University Data Protection Officer.

Unauthorised disclosure may be a disciplinary matter. If 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/ .

4.1.5 Research

The DPA 2018 and GDPR include some 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 http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf

5 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 Admissions in the case of applicants or to Registry in the case of students. 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 Responsibilities of employees as data subjects

All employees must ensure that any personal data supplied 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.

7 Disclosure outside of the European Union

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Personal data being processed by the University may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Further information is available from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/ .

8 Closed Circuit Television

The University uses Closed-Circuit Television as part of its security system. This is done in accordance with the CCTV Data Protection Code of Practice, issued by the Information Commissioner in 2017.

9 Subject Access Requests

The University complies with the individual right to access their personal data (subject access request) and information about how we do this is available on our website https://www.winchester.ac.uk/privacy-and-cookie-policy/

10 Further Information

The University of Winchester treats very seriously both the personal data and the sensitive personal data it processes on behalf its students and staff members, and also the wide range of other people with whom it has contact, and works.

For further information, contact the interim Data Protection Officer (Joseph.Dilger@winchester.ac.uk Tel: +44 (0) 1962 841515, Ext. 7670).

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