Information Management and Policy Services (IMPS)

University of Reading

Data Protection Policy

1. Purpose and scope

This policy applies to all University staff that handle personal data regardless of who created the personal data, where it is held, or the ownership of the equipment used to handle it.

1.1 This document sets out the University's policy on the handling of personal data.

1.2 The aim of the policy is to ensure that the University complies with its obligations under data protection legislation and that personal data is handled in line with the requirements of all data protection laws that protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

2. Definitions

Personal data	personal data is data about a living individual. That living individual must be identifiable, either directly or indirectly, through an identifier such as name, student number, email address, or online identifiers such as an IP address. For further guidance and examples, see Appendix A.
Processing data	means obtaining, recording, holding, sharing, and retaining and deleting of personal data and takes the same meaning as defined within data protection law.
GDPR	means the General Data Protection Regulation 2016/679 and the UK GDPR
DPA	means the Data Protection Act 2018
Data Protection Laws	means the GDPR, the DPA, the Privacy of Electronic Communications Regulations 2003 and any other applicable UK or international data protection laws that apply to processing of personal data by the University of Reading and its subsidiaries.
DPIA	means Data Protection Impact Assessments required under Article 35 of the GDPR
Data Subject Rights	means the right to be informed; the right to access; the right to object; the right to rectification; the right to restriction; the rights to erasure; the right to data portability and rights in relation to automated decision making and profiling.
DPO	means the Data Protection Officer
SIRO	means the Senior Information Risk Officer (the University Secretary)
IMPS	means the Information Management and Policy Services Office

Staff	**Includes:** - Employees (including temporary or short term workers) of the University or a subsidiary company of the University. - Volunteers, interns and those undertaking placements or work experience. - Contractors engaged by the University. - Students working for and/or on behalf of the University, including Post Graduate Research students. - Those with University accounts by virtue of a visiting or courtesy title conferred by the University. - Any other individual who is working on behalf of the University if they are processing personal data or information.
High Risk Data	means the categories of data described in Appendix B

3. Requirements

All staff:

- will be required to complete training in data protection.
- must always handle personal data in accordance with the data protection principles (see Appendix C) and the terms of this policy.
- are required to report an actual or suspected breach of data protection to the Data Protection Officer at imps@reading.ac.uk as required under the University Information Security Incident Response Policy.
- are required to notify the Data Protection Officer of data processing activities that may require a Data Protection Impact Assessment (DPIA) to be undertaken. A DPIA may be required if staff are considering new processing activities or setting up new procedures or systems that involve personal data. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative.
- are required to refer requests made under data subject rights (such as subject access requests) to the IMPS department promptly.
- must ensure that personal data are always held securely (with due regard to any additional safeguards required for High Risk Data) and are not disclosed to any unauthorised third party, either accidentally, negligently or intentionally, and must comply with the related policies set out in section 7 in this regard.
- will, wherever possible, consider applying anonymization or pseudonymisation where they are handling personal data, to reduce the privacy risks associated with handling personal data.

- will comply with any additional activity-specific data protection guidance issued by the University Data Protection Officer from time-to-time, including by way of example: guidance in relation to Data Protection and Marketing and Handling Research Data. Guidance will be made available at http://www.reading.ac.uk/internal/imps

- will ensure that appropriate written terms are in place before sharing personal data with any party outside the University, and/or before engaging any third party to perform any task or services that may involve the handling of personal data. Staff should liaise with IMPS or Procurement in this regard.

- must only process personal data in a manner that is consistent or compatible with the purpose(s) described in the applicable privacy notice.

- will not retain personal data for longer than is necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the personal data is no longer required it must be securely destroyed or deleted in accordance with the University's Records Management Policy.

4. Roles & Responsibilities

University's Policy Group	Implementation, monitoring and review of this policy.
Information Management and Policy Services	Ensuring training, guidance and advice regarding data protection compliance is made available to staff.
Data Protection Officer	Advising the University on its obligations, monitoring compliance, assisting with DPIAs and liaising with the Information Commissioner's Office.
Digital Technology Services Department (DTS)	Ensuring advice and guidance on technical specifications, such as encryption and DTS technical security measures is made available to staff.
Heads of Schools, Functions and Departments	Ensuring that their staff are made aware of this policy and that breaches of it are dealt with appropriately and developing and encouraging good information handling practices within their areas of responsibility.
Line Managers	Ensuring that their staff have completed all required training in Data protection
Information Asset Owners, Stewards and Custodians	Ensuring that information assets containing personal data are effectively managed in accordance with the data protection principles (described in Appendix C) and the

	terms of this policy.
University staff	- Complying with this policy. - Completing all required data protection training including refresher training. - Ensuring that they are processing data in line with University policies and requirements. - Ensuring that activities requiring a DPIA are referred to the Data Protection Officer. - Ensuring that requests made under data subject rights are referred to the IMPS team promptly. - Ensuring that suspected or actual compromises of personal data are reported to the IMPS team promptly.

5. Consequences of Non Compliance

4.1 Failure to comply with this policy can lead to

- damage and distress being caused to those who entrust us to look after their personal data, risk of fraud or misuse of compromised personal data, a loss of trust and a breakdown in relationships with the University.
- damage the University's reputation and its relationship with its stakeholders (including research funders and prospective students and collaborators).
- Significant legal and financial consequences. Monetary penalties of the Information Commissioners Office can reach up to 20 million euros or 4% of turnover. Individual civil action for breaches of data protection can also be taken by individuals or third party organisations where there is a failure to meet contractual obligations to hold data securely.

Failure to comply with this policy may result in us revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not the breach takes place at your normal place of work.

6. Guidance and Key Principles

The following key principles underpin this policy statement. All staff must comply with these principles.

- The contents of our systems and University data remain University property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for the University or on its behalf is the property of the University, regardless of who owns the device.
- University data held, including personal data, is subject to the Freedom of Information Act and data subject rights under the GDPR and DPA and must be provided to IMPS on request.
- The University will consider the requirements and rights under data protection laws when embarking on new data processing activities, procuring new services or suppliers, working collaboratively with external parties, and exploring new or innovative technical solutions for the processing of personal data.
- The University will factor requirements under data protection laws into project initiation stages, giving due regard to the balancing of available resources, system capabilities, technical compatibility and feasibility, and any additional measures in respect of security, accessibility and portability of personal data.
- Significant residual risks to personal data that remain after mitigation measures are put in place, including those highlighted by the Data Protection Officer, will be referred to the SIRO for consideration and approval.
- Due regard will be given to the protection of personal data at all times.

7. Related policies, procedures, guidelines or regulations

Key related policies and rules:

- Information Security Policy
- Regulations for the Use of the University of Reading's IT Facilities and Systems
- Encryption Policy (the Policy on Processing Personal Data and Sensitive Information off Campus or on an External Network)
- Records Management Policy
- Remote Working Policy
- Bring your own device (BYOD Policy)
- IT Equipment Disposal Policy
- Equal Opportunities Policy
- Information Security Incident Response Policy

Policies can be found at http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

8. Guidance and support

The University Data Protection Officer can be contacted via:

imps@reading.ac.uk

0118 378 8981.

9. Review

This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar
- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

Policies superseded by this policy

Data Protection Policy v1.1.2, 2.0, 2.1, 2.2, 2.3

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
2.0		IMPS	Aug 18	UoR Policy Group	Sep 18	Sep 18	Sep 19
2.1		IMPS	Sep 19			Oct 19	Oct 20
2.2		IMPS	Jan 21			Jan 21	Jan 23
2.3	9 Review Period updated	IMPS	Oct 22	UoR Policy Group		Oct 22	Oct 24
2.4	Reviewed, no changes	IMPS	Oct 24		Oct 24	Nov 24	Nov 26

APPENDIX A

Personal data

The following are examples of the types of data that can constitute 'Personal data':

***Name**

***Data of Birth/Age**

***Postal Address(es)** (to include postcodes)

***Contact telephone(s)**

***Email address(es)**

***Unique Identifiers** (to include: Student ID numbers, Staff ID numbers, Passport numbers, NHS numbers, National Insurance numbers, ORCID's, unique research participant ID numbers, Unique applicant ID numbers, vehicle reg, driving licence numbers)

***Images of individuals, including CCTV, photos**

***Location Data** (to include any GPS tracking data)

***Online Identifiers** (to include IP address data)

***Economic/financial data** (relating to an identifiable individual)

***Educational records** including but not limited to records held by the University and other education providers

***Counselling records**

***Pastoral records, including Extenuating Circumstances Forms**

***Disciplinary records**

***Training records**

***Employment records to include CV's, references**

***Nationality/Domicile**

***Ethnicity**

***Mental Health** (status, medical records conditions, to include disability)

***Physical Health** (status, medical records conditions, to include disability)

*__Dietary requirements__

***Sexual Orientation/Sexual life**

***Genetic Data** (to include DNA data)

***Biometric data** (such as facial image or fingerprint data)

***Political opinions**

***Trade Union membership**

***Religious or philosophical beliefs**

***Criminal Convictions and offences** (to include alleged offences and convictions)

APPENDIX B

High Risk Data

The following are examples of high risk personal data or sensitive information:

a. Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to, students, staff, alumni, research participants.

b. Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary

c. Information relating to 10 or more members of staffs' performance, grading, promotion or personal and family lives.

d. Information relating to 10 or more alumni/students' programmes of study, grades, progression, or personal and family lives.

e. Any set of data relating to 5 or more living, identifiable individuals' health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.

f. Information relating to identifiable research participants, other than information in the public domain.

g. Information that would be likely to disadvantage the University in funding, commercial or policy negotiations.

h. Information provided to the University in confidence.

i. Finance data held in Agresso and any payment card data covered by PCIDSS security requirements.

j. Health records of any living, identifiable individual.

k. Discussion papers and options relating to proposed changes to high profile University strategies, policies and procedures, such as the University's undergraduate admissions policy, before the changes are announced.

l. Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.

m. Information that would attract legal professional privilege.

APPENDIX C

Data Protection Principles

The data protection principles are that personal data must be:

(a) processed lawfully, fairly and in a transparent manner

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

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

(d) accurate and, where necessary, kept up to date

(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

(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