University of

Information Management and Policy Services (IMPS)

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 guidanc

- 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

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.

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

5.1 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

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)**

***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.

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