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 all data protection laws that protect the fundamen

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 indivi must be identifiable, either directly or indirectly, through an identif such as name, student number, email address, or online ident such as an IP address. For further guidance and examples, see Appendix A.
Processing data	means obtaining, recording, holding, sharing, and retaining an deleting of personal data and takes the same meaning as defi Regulations 2003 and any other applicable protection laws that apply to processing of University of Reading and its subsidiaries.
DPIA	means Data Protection Impact Assessments of the GDPR
Data Subject Rights	means the right to be informed; the right object; the right to rectification; the right to r erasure; the right to data portability and automated decision making and profiling.
DPO	means the Data Protection Officer
SIRO	means the Senior Information Risk Officer (t
IMPS	means the Information Management and Po

- 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 requirement for [illegible]

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 v1.1.2.0, 2.1, 2.22.3

Document control

VERSION

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