1. Introduction and Purpose

1.1 The University needs to collect, store, and use information about its staff, students, applicants, former students, and others in order to carry on its business as an institution of higher education and to meets its legal obligations to funding bodies and government. The purpose of this policy is to outline how the University meets its statutory obligations regarding Personal and Special Category (Sensitive) data.

2. Scope

2.1 This policy covers all Processing activities and supporting Information Systems involving Personal or Special Category Data where the University acts as the Controller.

2.2 This policy covers all global geographic territories, this includes Third Countries outside the UK and European Union (EU).

2.3 This policy applies to all personal information processed by the University in both electronic and physical record systems and should be followed by staff, students, contractors, third parties and anyone who processes Personal or Special Category Data on behalf of the University.

2.4 This policy takes precedence over any other University policy on matters relating to data protection.

3. Policy Statement

3.1 Royal Holloway, University of London (the University) is committed to ensuring the processing of Personal and Special Category Data relating to individuals is carried out in such a way as to protect the privacy of individuals and to comply with relevant legislation, in particular the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 and the Privacy & Electronic Communications Regulation 2003 ('PECR')

3.2 The 'UK GDPR' has six fundamental principles, all processing activities for and on behalf of the University shall be:

- Collected for specified, explicit and legitimate purposes only
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed lawfully, fairly and in a transparent manner
- Processed securely, in an appropriate manner to maintain security
- Adequate, relevant, and limited to what is necessary

3.3 Failure to comply with the principles of 'UK GDPR' may leave the University open to substantial fines.

3.4 The 'UK GDPR' also provides individuals with the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

3.5 Information about how to exercise these rights is located on the University's website.

4. Roles and Responsibilities

<u>Responsibilities of the University</u>

4.1 The University is the Data Controller as defined in the 'UK GDPR' and is ultimately responsible for the implementation of the regulation.

4.2 The University appoints a Data Protection Officer (DPO) who is the primary contact to the Information Commissioner's Office (ICO). This role is carried out in accordance with Articles 37-39 of the 'UK GDPR'. The Data Protection Officer is responsible for:

- Informing and advising the University of its data protection obligations
- Monitoring compliance
- Awareness-raising and training of staff
- Undertaking internal audits of data protection
- Providing advice on data protection impact assessments
- Cooperating with the Information Commissioner (ICO) and acting as the contact point for any issues relating to processing

Responsibilities of Staff

4.3 Heads of Departments and Professional Services are responsible for ensuring this policy is observed in their units and that staff complete Data Protection training as required.

4.4 Anyone who collects, stores, or uses personal data on behalf of the University must comply with data protection principles. Staff whose role requires them to process information about other people (including information connected with employment, academic study, or personal circumstances) must comply with the University's policies and procedures relating to data protection.

4.5 Staff who commission or employ third parties to process or handle personal data on behalf of or in connection with the University must ensure that the detail of such processing is subject to a written agreement that is compliant with 'UK GDPR between the University and the third party.

4.6 Personal data processed, hosted, or transferred outside the UK should be subject to additional safeguards and staff should seek appropriate advice before proceeding.

Responsibilities of Students

4.7 Students who are considering processing personal data as part of their programme must do so under the supervision of the member of staff responsible for their course. Students processing personal data, other than as part of their course, are required to make an individual notification to the Information Commissioner's Office.

Responsibilities of Council

4.8 Council members may receive confidential information that may include data that allows an individual to be identified. Independent members may be asked to serve on staff disciplinary hearings where they will learn of individual personal circumstances. All Council members will consider such information as confidential and the induction agenda for Council members will address this requirement.

5. Related Documents

5.1 This policy should not be read isolation. The following policies also include specific supporting requirements:

- UK GDPR and working from home
- UK GDPR and lecture recording
- Records Retention Policy
- Personal Data Breach Reporting
- Staff Email Usage Policy
- Information Security Policy
- Acceptable Use of Information Technology
- Research Ethics Policy
- Research Data Management Policy
- Code of practice in relation to releasing information to third parties

5.2 All related policies can be found on the University's Policy Hub webpages.

6. Monitoring and Compliance

6.1 The Executive Board will receive an annual report about how the University has responded to its obligations under the legislation.

6.2 Data Protection compliance will be reported at; the Audit, Risk and Compliance Committee (ARCC), Information Governance Committee (IGC) and Principals Advisory Group (PAG).

6.3 All suspected data breaches must be handled in accordance with the Personal Data Breach Procedure.

7. Definitions and Further Information

7.1 The following terms are defined in data protection legislation:

Personal data – any information relating to an identifiable person who can be directly or indirectly identified, by reference to an identifier (e.g., name, identification number, location data or online identifier).

Special category personal data – the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health related conditions (physical or mental health)
- Sex life and sexual orientation
- Commission or alleged commission of any criminal offence
- Genetic data
- Biometric data, where processed to uniquely identify an individual

Data subject – the individual to whom the personal data relates

Data controller – determines the purposes and means of processing personal data.

Data processor – responsible for processing personal data on behalf of a controller.

Data breach – a security incident that affects the confidentiality, integrity, or availability of personal data. A data breach occurs whenever any personal data is lost; corrupted; unintentionally destroyed or disclosed; accessed or passed on without proper authorisation; or made unavailable and this unavailability has a significant negative effect on the data subjects.

7.2 If anyone considers that this policy has not been followed, they should raise the matter with the Data Protection Officer.

7.3 Further information on the interpretation and application of this policy may be obtained from dataprotection@rhul.ac.uk

8. Document Control Information

8.1 The current official copy of this policy shall be located on the Policy Hub of the University's website.

Policy Owner *(usually Director-level)*	Data Protection Officer
Operational Owner *(where different to policy owner)*	
Approving Body	Executive Board
Approved on	16 February 2021
Reviewed	5th June 2023
To be reviewed before	5th June 2025

Version History		
Version (newest to oldest)	Date of approval	Summary of changes
V3.0	5.6.2023	'College' replaced with 'University' following change of status. Update to Related Documents

V2.0	16.2.2021	Update as a result of the UK leaving the EU. Additions include Related policies, principles of 'UK GDPR,' Definitions
V1.0	16.5.2018	Approved Issue