DATA PROTECTION POLICY

Policy last reviewed:	July 2026
Approved by:	Executive Board
Published on:	Royal Holloway University of London website

This Procedure is available in accessible formats on request from the [ ] team.

Please contact:

DATA PROTECTION POLICY

Royal Holloway, University of London

Version Number	Author	Purpose/Change	Date
V4.0	Data Protection Officer	Updated to reflect the Data (Use and Access) Act 2025, including the new right to complain to the University, changes to automated decision-making and references to responsible AI guidance; clarified accountability, complaints handling, related documents, DPIAs, partner and joint controller arrangements, and senior ownership and Executive Board accountability.	10 July 2026
V3.0	Data Protection Officer	'College' replaced with 'University' following change of status. Update to Related Documents.	5 June 2023
V2.0	Data Protection Officer	Update as a result of the UK leaving the EU. Additions include related policies, principles of UK GDPR, and definitions.	16 February 2021
V1.0	Data Protection Officer	Approved issue.	16 May 2018

Contents

1. Introduction and Purpose

The University needs to collect, store, and use information about its staff, students, applicants, alumni, research participants, visitors, contractors, and others in order to execute its business as an institution of higher education and to meet 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 Data and other data protection requirements.

2. Scope

This policy primarily covers Processing activities and supporting Information Systems involving Personal or Special Category Data where the University acts as the Data Controller. Where the University works with partners and another organisation is the Data Controller, or the parties act as joint controllers, data protection roles and responsibilities will be clearly defined, documented, and communicated to individuals where required.

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

This policy applies to all personal data 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.

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

3. Policy Statement

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, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') and the Data (Use and Access) Act 2025.

The 'UK GDPR' has six fundamental principles and an accountability requirement. 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
- Accountable, so the University can demonstrate compliance with the data protection principles.

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

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, including safeguards for significant decisions made solely by automated processing.
- The right to complain to the University about the handling of their personal data, and the right to complain to the ICO.

Information about how to exercise these rights is located on the University's website and in relevant privacy notices.

Individuals can raise concerns or complaints about the handling of their personal data by contacting the Data Protection Officer at dataprotection@rhul.ac.uk or via the University's published data protection complaints process available on the University website.

Under the Data (Use and Access) Act 2025, significant decisions made solely by automated processing may be permitted in wider circumstances, provided appropriate safeguards are in place. Where special category data is used, additional restrictions apply. Safeguards include providing information about the decision, enabling individuals to make representations, obtain human intervention, and contest the decision.

Where artificial intelligence or automated tools are used to process personal data, the University will do so in accordance with data protection legislation, this policy and relevant University guidance. Staff must ensure that any use of AI involving personal data is lawful, fair, transparent, secure, and subject to appropriate human oversight, risk assessment, and safeguards. Staff should also follow the University's responsible AI and guardrail guidance available through the AI Information Hub.

The University will provide a route for individuals to raise data protection complaints, acknowledge data protection complaints within 30 days, take appropriate steps to respond without undue delay, and tell individuals the outcome of their complaint. Individuals may complain to the ICO if they remain dissatisfied.

The University will carry out Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to individuals' rights and freedoms, in accordance with data protection legislation and University guidance.

4. Roles and Responsibilities

4.1 Responsibilities of the University

The University is the Data Controller as defined in the 'UK GDPR' and is ultimately responsible for the implementation of data protection legislation. The University, through its senior leadership, including the University Secretary, has overall responsibility for ensuring effective governance and oversight of data protection compliance.

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

4.2 Responsibilities of Staff

Faculty Deans and Heads of Professional Services are responsible for ensuring this policy is observed within their areas of responsibility, and that staff complete Data Protection training as required.

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.

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 the 'UK GDPR' between the University and the third party.

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

Staff must ensure that a Data Protection Impact Assessment is completed and approved where required before commencing high-risk processing.

4.3 Responsibilities of Students

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 and must follow relevant University guidance, research ethics requirements and instructions issued by the University. Students processing personal data other than as part of their course may have separate obligations under data protection legislation, including in relation to ICO registration where applicable.

4.4 Responsibilities of Council

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 or student disciplinary, grievance, appeal, or other formal panels where they will learn of individual personal circumstances. All Council members will consider such information as confidential, handle it securely and in accordance with this policy, and the induction agenda for Council members will address this requirement.

5. Related Documents

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

- Data Subject Rights procedure and published data protection information
- Data Protection Impact Assessment guidance and template
- Records Retention Policy and Records Management guidance
- Personal Data Breach Reporting Procedure
- Staff Email Usage Policy
- Information Security Policy
- Acceptable Use of Information Technology
- AI Information Hub, including responsible AI and guardrail guidance
- Research Ethics Policy and guidance
- Research Integrity guidance
- Research Data Management Policy
- Code of practice in relation to releasing information to third parties

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

6. Monitoring and Compliance

The Executive Board has overall accountability for ensuring that the University meets its data protection obligations and will receive regular reports on compliance, including an annual report about how the University has responded to its obligations under data protection legislation.

Data Protection compliance will be reported to the Audit, Risk and Compliance Committee (ARCC), Information Governance Committee (IGC), as appropriate.

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

7. Definitions and Further Information

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, for example 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.

If anyone considers that this policy has not been followed or has a concern about how their personal data has been handled, they should raise the matter with the Data Protection Officer (dataprotection@rhul.ac.uk) or use the University's published data protection complaints route on the University website.

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

8. Document Control Information

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

Policy Owner (usually Director-level)	Head of Legal Services
Operational Owner (where different to policy owner)	Data Protection Officer
Approving Body	Executive Board
Approved on	10th July 2026
Reviewed	30 June 2026
To be reviewed before	31 July 2029