Data Protection Policy

Policy Statement

Royal Holloway, University of London (the College) is committed to ensuring the processing of 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 General Data Protection Regulation (GDPR) and the Data Protection Act.

Scope

The College 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. All such information will be processed in accordance with the Data Protection principles that are set out in the GDPR.

This policy applies to all personal information processed by the College in both electronic and physical record systems and should be followed by staff, students, and anyone associated with the College in an official capacity.

Responsibilities of the College

The College is the Data Controller as defined in the GDPR and is ultimately responsible for the implementation of the regulation.

The College 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 GDPR.

Responsibilities of Staff

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.
Anyone who collects, stores or uses personal data on behalf of the College 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 College'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 College must ensure that the details of such processing is subject to a written agreement between the College and the third party.

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. 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

Independent members will be used to dealing with confidential and commercially sensitive information and in certain circumstances may receive confidential information that may include

data that allows an individual to be identified. They may also be asked to serve on student and 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.

Individual Rights

Under the GDPR, individuals have the following rights:

a) The right to be informed
b) The right of access
c) The right to rectification
d) The right to erasure
e) The right to restrict processing
f) The right to data portability
g) The right to object
h) Rights in relation to automated decision making and profiling.

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

Security

Staff and students alike must use appropriate organisational and technical measures to ensure that data is secure, to prevent disclosure, loss, and unauthorised access.

Further information regarding appropriate security measures can be found in the College's Information Security policies.

Monitoring and Reporting

The Planning and Resources Committee will receive an annual report about the ongoing operation of these procedures which must include:

a) confirmation of the annual notification to ICO.
b) a summary of related training and development activity across College
c) a summary and analysis of all data breaches over the past year
d) the number of all requests for access to personal data
e) an analysis of any complaints from individuals or ICO.

All suspected data breaches must be handled in accordance with the Data Breach procedures.

Further Information and Guidance

If anyone considers that this policy has not been followed they should raise the matter with the Data Protection Officer.
Further information on the interpretation and application of this policy may be obtained from dataprotection@rhul.ac.uk

Approved by:	PRC 16.05.18
Review by:	May 2023