Introduction

1. Royal Holloway, University of London (the College) is committed to ensuring the processing of information 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 Data Protection Act 1998 (DPA). 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 DPA.
2. This policy has been approved by the College Council and the Planning and Resources Committee. It forms part of the Data Management Policy, which ensures the College manages its data securely whilst maintaining data quality.

Responsibilities of the College

3. The College is the Data Controller as defined in the DPA and is ultimately responsible for the implementation of the Act.
4. The College appoints a Data Protection Officer (DPO) who is the primary contact to the Information Commissioner's Office (ICO) and is responsible for maintaining the annual notification to ICO. The DPO is also required to ensure there is a suitable DPA advisory and training service, for handling DPA subject access requests and for keeping the College Council and Secretary aware of relevant issues.

Responsibilities of Staff

5. Heads of Departments and Professional Services are responsible for ensuring this policy is observed in their units.
6. Anyone who collects, stores or uses personal data on behalf of the College must comply with the DPA 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 this policy and any associated guidelines.
7. Staff who process or access personal data must complete Data Protection training as part of their College induction and any refresher training as required by their line manager.
8. 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. Third parties include suppliers, partners or external examiners.

Responsibilities of Students

9. 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

10. 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 the student to be identified individually. 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 Data Protection Act 1998

11. Individuals have the right to access the data held about them, to ensure that it is correct and to know how it will be used.

12. All requests to access personal data will be handled in accordance with the DPA and as detailed in the Data Protection Guidelines. Requests should be directed to the Data Protection Officer.

Monitoring and Reporting

13. 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.

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

Further Information and Guidance

15. If anyone considered that this policy has not been followed they should raise the matter with the Data Protection Officer.

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

Approved by:	Council 06 07 2016
Review by:	July 2021