DATA PROTECTION POLICY

Owner:	University Secretary
Approver:	University Executive Board - 30 September 2025
Review due date:	September 2027
Current Version:	1.2
Update history:	v.1.1 – Approved by Council 14 October 2019 v1.0 – Approved by Council 12 March 2018
Document Type:	Strategic Policy
Classification:	Public

Data Protection Policy

1. Introduction

The University of Roehampton processes a wide range of personal data about individuals during the course of its day-to-day business and this processing is integral to many of the University's activities. The University also works with a number of third parties and external data controllers and processors. This policy sets out how such data will be used by the University to ensure that the various rights and obligations of all relevant individuals with respect to personal data are upheld and enforced. Any questions about this policy should be directed to the Data Protection Officer.

2. Scope of Policy

This policy applies to all members of the University, including staff, students, contractors, researchers and visitors, when they are processing personal data on behalf of the University. Its purpose is to ensure compliance with the UK GDPR and the Data Protection Act 2018, to safeguard the fair and secure use of personal data, to protect the rights of data subjects, and to protect the University against the risks that arise from the misuse of personal data.

3. Responsibilities

The University has a responsibility to implement appropriate and adequate provisions to ensure the proper use of personal data by its members. All individual members of the University, including staff and students, have a responsibility to comply with this policy and any other provisions relating to personal data. Failure by an individual member to comply with provisions made by the University to ensure the proper use of personal data, or with any of the obligations set out in this policy, or any other regulation, policy, process or procedure in respect of data protection, may result in disciplinary action being taken against the individual.

Individuals or groups have the following specific responsibilities under this policy:

3.1 The University Council

The University Council has ultimate responsibility for ensuring that the University complies with its legal obligations in respect of data protection and has delegated executive responsibility for the development and implementation of this policy and other provisions relating to data protection to the Vice-Chancellor and senior managers, and oversight of these arrangements to the Audit Committee.

3.2 Audit Committee

The Audit Committee will receive an annual report on data protection from the Data Protection Officer and will monitor risk with respect to data protection on behalf of Council. The Audit Committee will report relevant matters of data protection to Council as part of its regular reports.

3.3 Cyber and Data Protection Working Group

The Cyber and Data Protection working group will monitor implementation of policies and procedures and compliance with data protection legislation.

3.4 The Vice-Chancellor

The Vice-Chancellor has executive responsibility for the implementation of this policy and any other provisions relating to data protection. The Vice-Chancellor will ensure that adequate resources are available and systems are in place and that senior managers and other staff properly discharge their duties in relation to data protection. The Vice-Chancellor will provide adequate support to the Data Protection Officer in discharging their duties.

3.5 The Data Protection Officer

The University has appointed a Data Protection Officer to manage the implementation of the policy and other provisions relating to data protection on behalf of the University Council and the Vice-Chancellor.
The Data Protection Officer has the following responsibilities under this policy:

- To ensure the provision of adequate guidance and training to all University staff in respect of data protection
- To monitor the University's compliance with its legal obligations in respect of data protection
- To ensure the maintenance of all records demonstrating the University's compliance with its legal obligations in respect of data protection
- To provide advice on data protection to University staff, including advice on Data Protection Impact Assessments where required
- To act as the institutional point of contact and to ensure the University's co-operation

with the Information Commissioner's Office

The Data Protection Officer is authorised to conduct an audit of any area of the University to determine if this policy and any other provisions relating to data protection are being complied with. The relevant area will be given 30 days' notice of such an audit.
The Data Protection Officer will report directly to the Vice-Chancellor on all matters relating to personal data and data protection. The Data Protection Officer will consult with, but will not be instructed by the University Council, the Vice-Chancellor or any other member of staff in relation to their duties in respect of data protection.

The Data Protection Officer will not be penalised for properly discharging their duties under this policy or any other University provision relating to data protection.

3.6 IT Services

IT and Cyber Services, and in particular the Information Security Officer or individual vested with similar responsibilities, will provide technical support, advice and guidance to the Data Protection Officer in investigating and responding to data protection incidents and will assist in the development of solutions to prevent identified issues reoccurring. IT Services will also provide technical support, advice and guidance to staff to facilitate the embedding of privacy by design within the University.

3.7 All Managers

All University managers have the following responsibilities under this policy:

- To ensure that staff in their area of responsibility receive the appropriate training in respect of data protection
- To ensure that appropriate operational precautions and safeguards are implemented in respect of data protection
- To ensure that all data processing activities undertaken within their area of responsibility are compliant with this policy and any other University provisions relating to data protection
- To ensure that any data protection issues, including personal data breaches, are reported to the Data Protection Officer
- To ensure that any new systems or operations involving personal data processing are developed in line with the requirements of Section 14 of this policy
- To notify the Data Protection Officer of any changes to processing activities that will require an amendment of the Processing Activities Record (see Section 7)
- To co-operate with the Data Protection Officer in the discharging of their duties

3.8 All Staff

All University staff, including temporary staff, researchers, visitors and contractors, amongst others, have the following responsibilities under this policy:

- To comply with this policy and all other University provisions in relation to data protection
- To complete all required training within specified timescales
- To alert the Data Protection Officer and their line manager of any data protection issues or personal data breaches, and to comply with any subsequent instructions
- To take reasonable care to ensure that any work undertaken does not jeopardise the integrity of personal data
- To co-operate with the Data Protection Officer in the discharging of their duties

Failure to do so, particularly where this results in harm to other data subjects, may result in disciplinary action being taken.

3.9 Students

Students are expected to comply with this policy and any other University provisions relating to data protection. Failure to do so, particularly where this results in harm to other data subjects, may result in disciplinary action being taken under the Student Disciplinary Regulations.

3.10 Research Students and Staff

All University staff and students involved in research have the following specific responsibilities under this policy, in addition to those set out in paragraphs 3.8 and 3.9:

- To ensure that any personal data processing undertaken for research purposes is done so in a way that is compliant with this policy and any other University provisions for personal data
- To comply with the guidance set out in Data Protection for Researchers
- To complete all required training within specified timescales
- To co-operate with the Data Protection Officer in the discharging of their duties

4 Definitions

The following definitions are used throughout this policy, and have been adapted from the relevant legislation:

Anonymisation	Personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. Data protection law does not apply to data that has been rendered anonymous.

Controller	The person or organisation that determines the purposes and means of the processing of personal data.
Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
Personal data	Any information relating to an identified or identifiable person (a 'data subject') or from which a person can be identified either directly or indirectly. Examples include: - Name - Age - Address - ID number - Financial information - Assessment information - Employee performance evaluations Personal data includes an expression of opinion about a person and an expression of the intentions of the University in respect of that individual.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data. This includes, but is not limited to the collection, recording, organisation, storage, alteration, use or disclosure of personal data, or otherwise making personal data available.
Processor	The person or organisation that processes personal data on behalf of a controller.
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. Data protection law places less onerous restrictions on personal data that has been pseudonymised
Special categories of personal data	Personal data relating to the following characteristics of a data subject: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Health - Sex life - Sexual orientation - Genetic data - Biometric data (where used for identification purposes)

5 Associated documentation

The following documents have been developed in association with this policy, and are referred to throughout:

- Data Protection for Researchers, including students carrying out research
- Information About Personal IT Security
- University Record Retention Schedule
- Personal Data Breach Procedure

6 Data protection principles

The General Data Protection Regulation sets out a number of principles relating to the lawful processing of personal data, which the University and its members must comply with. These are as follows:

Lawfulness, fairness and transparency	Personal data will be processed lawfully, transparently and fairly in relation to the data subject.
Purpose limitation	Personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with this, unless further processing is in the public interest, or is for scientific or historical research purposes, or for statistical purposes.
Data minimisation	Personal data collected will be adequate, relevant and limited to what is necessary to fulfil the purpose of the processing.
Accuracy	Personal data will be accurate and kept up-to-date.
Storage limitation	Personal data will be kept in a form enabling identification of the subject no longer than is necessary to fulfil the purpose for which it was collected in the first place, unless retaining it beyond this point is in the public interest, or is for scientific or historical research purposes, or for statistical purposes.
Integrity and confidentiality	Personal data will be processed to ensure against unauthorised or unlawful processing, accidental loss, destruction or damage.

7 Data Protection Training

The University is committed to ensuring that all members of staff receive adequate data protection training. It is mandatory for members of staff to complete data protection training and to renew this training as required.

8 How personal data is used by the University

The University maintains a record of its processing activities (Record of Processing Activities) as a controller or processor, which is maintained by the Data Protection Officer. It is the responsibility of the manager who oversees a particular personal data processing activity to notify the Data Protection Officer if any changes need to be made to the Record of Processing Activities.

The University will process personal data in line with the data protection principles outlined above and will only do so where there is an identifiable legal basis from the following list.

- The data subject has given the University their consent
- The processing is necessary for the performance of a contract between the University and the data subject
- The processing is necessary for the University to meet its legal obligations
- The processing is necessary to protect the vital interests of a data subject or other person
- The processing is necessary for the University to perform a task in the public interest or to exercise its official authority
- The processing is necessary in the pursuit of the legitimate interests of the University or a third party unless the rights and freedoms of the data subject override these interests

There may be circumstances in which the University seeks to use personal data for a purpose other than that for which it was collected. Where this is the case, the University will consider the following before engaging in the alternative processing activity:

- Any links between the purpose for which the data was originally collected and that of the proposed alternative processing
- The context in which the personal data was collected
- The nature of the personal data
- The possible consequences of any further processing
- The existence of suitable safeguards

Data subjects will be provided with information about the nature of the processing activity, the legal basis on which it is conducted, and their rights in respect of that activity in line with Section 12 below.

9 Data subject rights

Depending on the nature of the data processing activity, data subjects may have one or more of the following rights with respect to their personal data.

Data subjects should contact the Data Protection Officer (DataProtectionOfficer@roehampton.ac.uk) to discuss or make a request in respect of any of these rights.

9.1 Right of access

Where it is acting as a controller, individuals have the right to obtain from the University confirmation of whether or not their personal data are being processed, and if so, access to the personal data and the following information:

- The purpose of the processing
- The categories of personal data concerned
- The recipients to whom the personal data have been or will be disclosed
- The period for which the personal data will be stored
- Where the data are not collected directly from the data subject, any available information about their source
- Whether the data are used for automated decision-making, including profiling, and if so, details about such processing

9.2 Right to data portability

A data subject may request to receive personal data in a commonly used format that allows them to transmit the data to another controller. This right does not apply where the processing is in the public interest or is necessary for the University to exercise its official authority.

9.3 Right to rectification

Data subjects have the right to ask for any inaccurate personal data held by the University to be corrected, and any incomplete data to be completed. In the case of incomplete data, the University may request a supplementary statement from the data subject.

9.4 Right to be forgotten ('erasure')

A data subject has the right to request that the University erases any of their personal data in the following circumstances:

- The data is no longer required to fulfil the purpose for which it was collected
- Where the processing is based on consent and this is withdrawn, and where there are no other legal grounds for processing
- Where the subject objects to the processing under Section 8.6
- Where the data is being unlawfully processed
- Where the data has to be erased to comply with the University's legal obligations
- Where the data was collected in relation to the offer of information society services

directly to a child

The University may decline to erase the data where it considers that the processing is necessary for the following reasons:

- To exercise the right of the University or any of its member to freedom of expression and information
- To comply with the University's legal obligations, or where the processing is in the public interest or is necessary for the University to exercise its official authority
- For public interest reasons relating to public health
- For archiving purposes in the public interest, for scientific or historical research, or for statistical purposes, to the extent that complying with the right would make the purpose of the processing too difficult to achieve
- To establish, exercise or defend legal claims

Where the University has transferred this data to a third party, it will take reasonable steps to notify the third party that the data should be erased.

9.5 Right to request a restriction of processing

A data subject has the right to request that the University restricts processing of their personal data in the following circumstances:

- The accuracy of the data is contested by the subject, in which case the restriction applies for a period sufficient to enable the University to verify the accuracy of the data
- The processing is unlawful and the data subject prefers a restriction to processing over erasure
- The University no longer needs the data for processing, but the data subject needs it to establish, exercise or defend legal claims
- The data subject has objected to the processing pending verification as to whether the legitimate grounds of the University override their rights

Where a legitimate request to restrict processing is made, the University may nevertheless continue the processing activity in the following circumstances:

- To establish, exercise or defend legal claims
- To protect the rights of individuals
- For public interest reasons

9.6 Right to object to personal data processing

A data subject may object to a processing activity if the processing is based on the following:

- The public interest
- The exercise of official authority or the legitimate interests of the University

The University will stop the processing unless there are compelling and legitimate reasons to do so or in the interests of establishing, exercising or defending legal claims.
Where data is used for direct marketing purposes, a data subject may object to the processing at any time, in which case the University will cease using the data for this purpose.

Where data is processed for scientific, historical or statistical purposes the subject can object to processing on grounds related to their personal circumstances unless the processing is in the public interest.

9.7 Rights regarding automated individual decision-making, including profiling

A data subject has the right not to be subject to a decision based on purely automated processing which has a significant or legal effect on them. This right does not apply if the decision:

- Is necessary to enter into a contract between the University and the data subject
- Is authorised by law

10 Sharing of Personal Data

University staff should only share personal data with another employee if the recipient has a job-related need to know the information.

The University will not share personal data with external third parties unless there is a lawful basis to do so. Generally, the University will not share personal data externally unless a Data Sharing Agreement is in place with the third party, although it may do so in certain circumstances where this is legal, for instance if the sharing of data is required for law enforcement or safeguarding reasons, or to protect the vital interests of the data subject.

Where teams within the University have Standard Operating Procedures for the sharing of personal data, these should be adhered to at all times.

11. Special categories

'Special categories' of personal data are defined above. In accordance with Article 9 of the UK GDPR, the University will only undertake processing activities relating to special categories of personal data in the following circumstances:

- The data subject has given explicit consent

- The processing is necessary to exercise the rights or obligations of the University with respect to employment, social security or social protection law
- Processing is necessary to protect the vital interests of the data subject where they are incapable of giving consent
- Processing is carried out in the course of the legitimate activities of the University, as a not-for-profit body, with respect to its own members, former members or persons with whom it has regular contact in respect of these activities
- The data subject has already made the data public
- The establishment, exercise or defence of legal claims
- Processing is in the public interest
- Processing is necessary for the purposes of preventative or occupational medicine
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving in the public interest, for scientific or historical research purposes, or for statistical purposes.

12. Research

The University has developed a mechanism for assessing the data protection implications of using personal data for research, which is integrated with the research ethics approval process.

The University also provides high-capacity, secure data storage facilities, which all researchers are expected to use during the course of their research. Any derogations from this should be authorised by the Data Protection Officer.

Supplementary guidance and information exists for researchers in respect of personal data: Data Protection for Researchers.

13. Provision of information

Where it is acting as a controller, the University will provide data subjects with the following information, in the form of a privacy notice, at the time the personal data is obtained:

- Confirmation that the University is acting as personal data controller
- Contact information for the Data Protection Officer
- The purpose and legal basis for the personal data processing, and whether provision of the information is optional or mandatory
- Details of any third parties who will have access to the data and, if the data is to be sent outside of the European Economic Area the location to which it will be transferred
- How long the data will be stored for
- Whether the data will be used for automated decision making
- The rights of the data subject as set out in Section 8 of this policy
- The right of the data subject to make a complaint to the Information

Commissioner's Office, as set out in Section 16 of this policy

There may be circumstances where the University becomes the controller of personal data that it did not collect directly from a data subject. In such circumstances, the University will provide the data subject with the above information, as well as information about where the data originated from. The University will provide this information to the data subject within one month of receipt of the data, when it first communicates with the data subject, if the data is to be used to communicate with the data subject, or if the data is disclosed to a third party, whichever occurs soonest.

If the data is to be used for a purpose other than that for which it was originally collected, the University will inform the data subject of this and the additional purpose of the processing.

The University has developed a Privacy Notice Template (available from the Data Protection Officer) to assist in the provision of information to data subjects.
The data subject will be given an opportunity to request the above information in an alternative, accessible format.

14. Record retention

In line with the principles outlined in Section 3 above, the University will retain all personal data in line with the University Record Retention Schedule. The University will provide the Data Subject with specific information about how long it will keep the personal data at the point of capture, in line with Section 12. The University may retain personal data beyond the point originally specified where it is in the public interest to do so, or where this is required for scientific, historical research or statistical purposes. Where personal data is retained beyond the point originally specified, the University will ensure that appropriate technical and organisational measures are in place to uphold the principle of 'data minimisation' as set out in Section 3. This may include subjecting personal data to a process of anonymisation or pseudonymisation, details of which can be found in the following documents: Data Protection for Researchers.

15. Privacy by design

The University is committed to the principle of 'privacy by design' in respect of its personal data processing activities. Accordingly, it will ensure that appropriate technical and organisational measures are in place to safeguard personal data and to implement the data protection principles set out in Section 3. The University has developed the following guidance to assist its members in undertaking operational activities involving personal data: Data Protection for Researchers. This guidance includes information about how to anonymise or pseudonymise personal data in a way that is compliant with the University's legal obligations.
Where a new activity or operation is developed that may involve a high risk to data

subjects the University is legally required to carry out a Data Protection Impact Assessment before processing can begin.
If it is deemed possible that a project could cause a higher risk to data subjects, the manager responsible should carry out an initial screening process to determine whether a full DPIA is needed, using the DPIA Screening Form. Factors which may pose a higher risk include:

- Processing of personal data on a large scale, for example introducing a new system for managing student records;
- processing of special category personal data or data relating to criminal offences;
- sharing of data with external parties, especially those outside the European Economic Area;
- any automated processing of personal data;
- any novel method of processing personal data, such as use of Artificial Intelligence, on a large scale.

The manager must submit the completed screening form to the Data Protection Officer. If the requirement to carry out a full DPIA is triggered, the DPO or their nominee will work with the manager to complete this. Once the DPIA is completed, the DPO will make the final decision as to whether the risks identified can be sufficiently mitigated for the processing to proceed. Completed DPIAs will be kept on file and reviewed regularly to ensure risks are managed appropriately and any changes to data processing are reflected.

16. Personal data breaches

Where it is suspected that a data breach has occurred, members of staff should inform their line manager and report the incident to the Data Protection Incident inbox, UOR-DPI@roehampton.ac.uk immediately. Students should inform their Tutor, who will report the suspected breach to their line manager and the make notification to the Data Protection Incident inbox

The University strives to ensure that personal data is processed safely and securely, but it is also essential that appropriate processes are in place should this safety and security be compromised at any point and should a personal data breach occur.
Where a breach occurs that is likely to result in a risk to the rights and freedoms of a person, the University as data controller may be required to report the breach to the Information Commissioner's Office within 72 hours of its occurrence. It is also the responsibility of the University as data controller to make a report to the ICO in cases where a third party is processing data on its behalf.

Where a breach is likely to result in a high risk to the rights and freedoms of a person, the University as data controller may be required to report the breach to the person in question. The Data Protection Officer is solely responsible for deciding whether a report should

be made to the ICO and/or to the person in question, and for communication of the relevant information as required.

In cases where the University is acting as the data processor, it will report any personal data breaches to the relevant data controller without undue delay.

The University has developed a Personal Data Breach Procedure for dealing with personal data breaches. It is the responsibility of all members of the University to familiarise themselves with and adhere to this procedure.

17. Making a complaint

The University endeavours to ensure that all personal data for which it is responsible is handled in an appropriate manner. If you have any concerns about the University's handling of personal data, then please contact the University's Data Protection Officer.

All data subjects have the right to make a complaint about the University's handling of personal data to the Information Commissioner's Office and can do so at https://ico.org.uk/concerns/.