REGENT'S
UNIVERSITY LONDON

Data Protection Policy

Owner:	*Director of Governance, Legal & Strategic Projects*
Approved by:	*VCET (Vice Chancellor's Executive Team)*
Approval date	*August 2022*
Review date:	*January 2026*
Next review due date:	*3 years or as required.*
Version:	*2.0*
Policy reference number	*Gov 01*

If you require this document in an alternative format please contact the Disability Officer on 020 7487 7863 or email disability@regents.ac.uk

Policy version tracking

Version Number	Date	Revision Description	Editor	Status
1.5.	Jan-18	Darren Tysoe - CIO	Changes incorporated under the General Data Protection Regulations (GDPR).	Published
1.6.	Jan-18	Darren Tysoe - CIO	Amended to include ‘Clean desk principles’ (section 5.5)	Published
1.7.	Apr-18	Darren Tysoe - CIO	Amended to replace governance email address with privacy	Published
1.8.	July 2021	Richard Reger – Head of Governance	Amended to reflect changes to legislation and Open University Audit recommendations	Published
1.9.	Aug 2022	Aoife McGuinness - Head of Governance	Review in line with SAR procedures and forms	Published
2.0	January 2026	Clare Kane, Director of Governance, Legal & Strategic Projects	Update to Accountable roles and responsibilities. Minor updates to operational statements.	

REGENT'S
UNIVERSITY LONDON

Data Protection Policy

The UK General Data Protection Regulation (UK GDPR) to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020).

Regent's University London recognises its responsibilities in protecting the rights of individuals' personal data. The purpose of this policy is to ensure that Regent's, its employees and students, comply with the provisions of the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

This policy applies to all personal data handled by Regent's employees, students and other authorised individuals, in all formats including paper and electronic files, on computers and mobile devices and regardless of who owns the device on which it's stored. Any infringement of the Act will be treated seriously by Regent's and may be considered under disciplinary procedures. Serious breaches may also result in Regent's or the employee or student concerned being held liable in law.

This Policy identifies and explains the data protection roles and responsibilities and sets out a list of the requirements that employees, students and others must comply with. Regent's retains the right to change this policy at any time.

1. Definitions

1.1 Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. An example where Regent's acts as data controller is in relation to the processing of employee data.

1.2 Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller.

1.3 Processing refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

1.4 Data Subject refers to the identifiable natural person whose personal data is processed by a data controller and/or data processor or on their behalf. Examples of data subjects are students, employees and alumni or past students.

1.5 Personal data means any information relating to a living individual who can be identified directly or indirectly from the data and other information.

1.6 Special categories of personal data are more sensitive and requires additional protection, including health or medical information, race, ethnic origin, political opinions, religious or similar beliefs, trade union memberships, sexual life or orientation information, criminal convictions/offences and genetic or biometric data.

1.7 Confidential data is that given in confidence, or with an agreement for it to be kept confidential. Some confidential data will also be special category data and will come within the terms of this policy.

2. Responsibilities

2.1 The Data Controller

Regent's University London Limited is the data controller under the Act. The Board is ultimately responsible for compliance with the Act. The Vice-Chancellor's Executive Team (VCET) is responsible for the strategic implementation of the Data Protection Policy. Specific responsibilities are set out below:

Data Protection Officer ('DPO')	The DPO is responsible for: advising on the obligations of Regent's University London and its employees; monitoring compliance with the Regent's University Data Protection Policy including awareness raising and co-operating with the supervisory authority; advising on data protection impact assessments ('DPIAs'). Any questions about the operation of this Policy or any concerns about compliance with Data Protection Laws should be referred in the first instance to the DPO. The DPO role for the University is held by the Director of Governance, Legal & Strategic Projects.
Chief Financial Officer	The Chief Financial Officer has ultimate accountability for maintaining compliance with Data Protection Laws through the application of appropriate governance and contractual frameworks.
Data Privacy & Information Security Group	The Data Privacy and Information Security Group is authorised by the Vice Chancellors Executive Team. It is comprised of subject matter expert roles responsible for overseeing the implementation of internal governance, policies and procedures to achieve University compliance with applicable Data Protection Law, Information Security and Business Continuity best practice. The Data Privacy & Information Security Group is comprised of departmental representatives whose role is to assist the Data Protection Officer and ITS Director in the implementation of this policy within their department: raising general awareness of data protection matters; assisting with data protection related incidents; assisting in the management of local breaches and implementation of mitigating action.
Associate Provosts, Head of Schools, Heads of Departments	Associate Provosts and Professional Services Department Heads have accountability for maintaining compliance with Data Protection Laws in relation to their department or academic area. They must ensure the practical implementation of this policy through appropriate operational procedures, including maintaining up-to-date Processing Records for their respective areas and ensuring Third Parties who handle data on the university's behalf are compliant with the university's requirements.

Chief Information Officer	The Chief Information Officer has accountability for maintaining compliance with Data Protection Laws through the application of appropriate technical security measures and operational procedures to protect personal data which is held electronically.
Deputy Vice Chancellor & Provost	The Deputy Vice Chancellor & Provost is accountable for ensuring that the academic research process and the Research Ethics Panel is managed in compliance with Data Protection Laws. They must ensure the practical implementation of this policy through appropriate operational procedures and ensure research data is processed in compliance with Data Protection Laws.
Employees	Each employee has personal responsibility for their own handling of personal data of applicants, students, alumni, employees, suppliers and other third parties. This includes ensuring compliance with the University's data privacy procedures and following retention guidelines. Further detail is set out in 2.2.
Third parties including Suppliers	All Third Parties and Suppliers must ensure: Personal information processing is compliant with the requirements as set out in the contract between the third party supplier and Regent's University London; a nominated data privacy contact and sufficient resource is in place with the necessary skills and knowledge developed and maintained to discharge data privacy accountability under the contract; risk based monitoring plans are established and embedded; data privacy risks, incidents or Policy breaches are reported to Regent's University London within 48 hours of identification to action appropriate remediation and regulator engagement.

2.2 Employee Responsibilities

All employees shall:

- Ensure the processing of personal data in all formats is compatible with the Data Protection Act;
- Raise any concerns in respect of the processing of personal data with the DPO;
- Promptly pass on to the DPO any individual requests made under the 'rights of the data subject' as set out in data protection legislation, including Subject Access Requests (SARs) and authorised access requests from third parties for personal data (e.g., Police);

- Where employees are sharing and processing personal data with other organisations, they must ensure appropriate data sharing and processing agreements are in place;
- Ensure that all personal information which they provide to Regent's in connection with their employment is accurate and up-to-date;
- Inform Regent's of any changes to information, for example change of address;
- Check the information Regent's makes available from time to time, in written or automated form, and inform Regent's of any errors or, where appropriate, follow procedures for updating entries on computer forms. Regent's shall not be held responsible for errors of which it has not been informed;
- Complete mandatory data protection training, as required.

When employees hold or process information about students, colleagues or other data subjects (for example, students' coursework, references to other academic institutions, or details of personal circumstances), they should comply with the following guidelines and also their responsibilities under related policies, including, but not limited to, the IT Acceptable Use Policy. Employees shall ensure that:

- All personal information is kept secure;
- Personal data is kept in accordance with Regent's retention schedule;
- Data security incidents, losses, near misses or unauthorised disclosures of personal data are reported immediately to the attention of the DPO and that they support the DPO in resolving breaches; and
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. Unauthorised disclosure may be a disciplinary matter, and may be considered gross misconduct in some cases.

When employees supervise students doing work which involves the processing of personal information, they must ensure that those students are aware of the data protection principles, in particular, the requirement to obtain the data subject's consent where appropriate.

Employees should adhere to clean desk principles as it reduces the threat of sensitive, confidential or personal data being stolen. Action should include:

- At extended periods away from a workspace such as lunch breaks and at the end of the working day, staff should remove documents from desks that contain sensitive, confidential, or personal information and placing in a locked drawer or filing cabinet.
- Portable devices such as laptops and tablets should be locked away when not in use and protected with passwords and encrypted.
- Confidential waste must be disposed of in accordance with the appropriate internal procedures for confidential waste.
- Locking/logging off from devices when away from the desk.

Line managers must ensure that they and employees reporting to them understand the implications of data protection legislation for the way they process personal data and seek advice from the DPO if in doubt.

2.3 Student Responsibilities

All students shall:

- Familiarise themselves with the Data Protection Agreement provided when they enrol;

- Ensure that all personal information which they provide to Regent's is accurate and up-to-date;
- Inform Regent's of any changes to that information, for example changes of address; and check the information which Regent's make available from time to time, in written or automated form, and inform Regent's of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. Regent's shall not be held responsible for errors of which it has not been informed;
- If students process personal information (for example, in coursework or research), they must comply with the requirements of processing personal data in accordance with UK GDPR legislation.
- All students shall successfully complete the required information compliance training before processing personal data for the purposes of their study.

3. Legal basis for processing information

3.1 Regent's holds and processes information about employees, students, alumni, contractors, users of its services and other data subjects for academic, administrative and commercial purposes. In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

- The data subject has given consent for their data to be processed for a specific purpose.
- The processing is required due to a contract.
- It is necessary due to a legal obligation.
- It is necessary to protect someone's vital interests (i.e., life or death situation).
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- It is necessary for the legitimate interests of the controller or a third party, and it has been established that the need to protect individuals' personal data does not override those interests.

3.2 For special categories of personal data, at least one of the following conditions must be met:

- The data subject has given explicit consent.
- The processing is necessary to comply with the law and in the interests of the individual.
- The processing is necessary to protect vital interests of the individual and the individual is incapable of giving consent.
- The processing is manifestly made public by the data subject.
- Data about criminal convictions and offences can only be processed if there is specific legal authorisation to do so. Please consult the DPO for advice about processing special category data.

3.3 Once a legal basis for processing has been established for handling such information, Regent's, and all employees or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the Act) and UK GDPR. In summary these state that personal data shall:

- Be processed fairly, lawfully, and in a transparent manner;
- Be collected for specified, explicit and legitimate purposes and shall not be processed in any manner incompatible with those purposes;
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Be accurate and, where necessary, kept up-to-date;

- Not be kept in a form which permits identification of data subjects for no longer than necessary for the purpose; and
- Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Rights of individuals

4.1 UK GDPR aims to strengthen the rights of individuals when processing their personal data:

- 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; and
- The right not to be subject to a decision based solely on automated processing, including profiling.

4.2 Information for individuals on how to request rectification, erasure, restriction of personal data and how to object to processing of personal data will be available from the DPO. Regent's will take reasonable steps to verify the requestor's identity before being able to process a request. Once ID is verified, Regent's will consider and action such requests free of charge, unless the request is repetitive or onerous, in which case a fee may be charged based on the administrative cost of locating and rectifying the information. Regent's aims to do this within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request. When requests are made regarding large quantities of information, Regent's will ask the individual to specify the information required. Regent's may refuse the request if it is manifestly unfounded or excessive, giving reasons for refusal. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request. If the data has been shared with other organisations, Regent's will take action to inform these organisations.

5. Rights to Access Information

5.1 Employees, students and other data subjects at Regent's have the right to access any personal data that is being kept about them, either on a device or in structured and accessible manual files. Any person may exercise this right by following the guidance in the Subject Access Request Procedure and Subject Access Application Form which are available on the website. The request should be submitted with ID verification to the DPO at governance@regents.ac.uk.

5.2 Entitlement under Article 15(1) of the UK GDPR is to receive access to information in so far as it constitutes the requestor's 'personal data' of which Regent's is the controller, having conducted a reasonable and proportionate search. The requestor is not entitled to receive information regarding Regent's or its employees or management, unless it constitutes the requestor's personal data. Regent's is entitled to withhold certain information from the response to a Data Subject Access Request where one or more exemptions under the Data Protection Act 2018 apply.

5.3 Regent's aims to comply with requests within one month of receipt of the Data Subject Access Request, starting from the day after the request is received by the DPO, or the day on which proof of identification is received and verified. Regent's aims to do this within one month of receipt of the request, unless requests are complex or numerous. In such cases, there may be an extension of up to two months and the individual will be informed and reasons given within a month of the request.

Regent's will take reasonable steps to verify the requestor's identity. If Regent's process a large amount of information about an individual, it may need to ask the data subject to provide additional information to help clarify their request.

5.4 Regent's will usually provide a copy of the information free of charge. However, should the request be considered excessive, repetitive or unfounded, Regent's may refuse the request. Individuals may complain to the Information Commissioner's Office if they are not satisfied with the refusal of a request. If there is a vast amount of data requested, Regent's may charge a fee based on the administrative cost of locating, rectifying and providing the information.

5.5 Students are entitled to information about their marks for assessments. There is nothing to prevent academic staff from meeting with students to provide feedback, including showing them the assessment and/or providing the comments which they relate to. Regent's therefore encourage academics to do this, rather than ask the student to make a formal subject access request for the information. Students are therefore advised, in the first instance, to contact their tutor for this information.

6. Documentation and safeguards

6.1 Regent's shall maintain a record of all the types of personal data held and processed, and the reasons for which it is processed. This record will be held by the Data Protection Officer (DPO). Under the GDPR and the DPA, Regent's has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy. The information which is currently processed by Regent's and the purposes for which it is processed are set out in the Privacy Notice available on the website for students, and the GDPR - HR Employee Privacy Notice and GDPR - HR Record of Processing Activity for employees. These may be updated from time to time.

6.2 Consent

Where we rely on consent as the lawful basis for processing personal data, we will ensure that consent is freely given, specific, informed, and unambiguous. Consent will be obtained through a clear affirmative action and will be recorded. Data Subjects have the right to withdraw their consent at any time, without detriment, by contacting the DPO. Withdrawal of consent will not affect the lawfulness of processing carried out before consent was withdrawn.

6.3 Processing of Special Category Personal Data

Special category personal data includes information revealing racial or ethnic origin, religious or philosophical beliefs, data concerning health, or data concerning a person's sex life or sexual orientation.

We will only process special category personal data where a lawful basis under Article 6 of the UK GDPR applies and one of the specific conditions in Article 9 of the UK GDPR is met. These conditions may include, for example, where the data subject has given explicit consent, where processing is

necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment, where processing is necessary to protect vital interests, or where processing is required for reasons of substantial public interest as set out in the Data Protection Act 2018.

We apply appropriate technical and organisational measures to safeguard special category personal data and ensure it is accessed only by authorised individuals on a need-to-know basis. We retain such data only for as long as necessary to fulfil the purposes for which it was collected and to meet applicable legal or regulatory requirements.

6.4 Data protection impact assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted if required. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce privacy risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an afterthought.

6.5 Transfers of personal data internationally

Personal data can only be transferred out of the UK when there are safeguards in place to ensure an adequate level of protection of the data. All instances of overseas transfers of personal data must be subject to appropriate technical safeguards and contractual provisions incorporating appropriate assurances to ensure the security of the data is fully compliant with the UK's data protection legislation.

6.6 Direct marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For Regent's, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003 (PECR). Regent's must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

6.7 Retention and disposal of data

Regent's will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements. Personal information is retained for no longer than the periods permitted in Regent's retention schedule. Out of retention information will be destroyed securely, for example by shredding or appropriate electronic erasure.

6.8 HESA data collections

Data about students will be supplied to the Higher Education Statistics Authority. The full HESA Data Collection Notice is available from this link: http://www.hesa.ac.uk/fpn.

7. Compliance

7.1 Compliance with the Act and UK GDPR is the responsibility of all students and employees. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the DPO by email to governance@regents.ac.uk.

7.2 Any individual, who believes that the policy has not been followed in respect of personal data about themselves, should raise the matter with Regent's as the data controller initially. If the matter is not resolved, you should refer to the grievance procedure for employees, the complaints policy and procedure for students or initiate. If you remain dissatisfied after following these steps, you can complain to the Information Commissioner's Office (ICO). You should do this within two months of receiving Regent's final response to your complaint. For further advice on making a complaint to the ICO, please see their website at www.ico.org.uk.

8. Related Documents

8.1 This Data Protection Policy should be read in conjunction with the following policies and procedures:

- IT Acceptable Use Policy
- Remote Access Policy
- Information Systems Security Policy
- Computer Monitoring Policy
- Subject Access Request Procedure
- Subject Access Request Form