REGENT'S
UNIVERSITY LONDON

Data Protection Policy

Owner:	*Head of Governance*
Approved by:	*VCET (Vice Chancellor's Executive Team)*
Approval date	*Date: July 2021*
Review date:	*July 2021*
Next review due date:	*June 2022*
Version:	*1.8.*
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

Table of Contents

REGENT'S
UNIVERSITY LONDON

1. Introduction

1.1. Regent's University London recognises its responsibilities with regard to the management of the requirements of the Data Protection Act 2018, and UK General Data Protection Regulation (UK GDPR).

1.2. The purpose of this policy is to ensure that the University and the University's staff and students comply with the provisions of the Data Protection Act 2018, and UK GDPR when processing personal data. Any infringement of the Act will be treated seriously by the University and may be considered under disciplinary procedures.

1.3. This policy applies regardless of where the data is held, i.e. if it is held on personally-owned equipment or outside University property.

1.4. This Policy:

- sets out the data protection principles that underpin the privacy framework;
- identifies and explains the data protection roles and responsibilities; and
- sets out a (non-exhaustive) list of the requirements that employees mustcomply with.

2. The Principles

2.1 Processing information

Regent's University London holds and processes information about employees,students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the University, and all staff or otherswho 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 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.

2.2 GDPR Rights

GDPR aims to strengthen the rights of individuals. The individual data protectionrights under GDPR are:

- 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.

2.3 Conditions of processing/lawfulness

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

- The data subject has given consent.
- 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.

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 for the purposes of employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests.
- The processing is carried out by a not-for-profit body.
- The processing is manifestly made public by the data subject
- The processing is necessary for legal claims
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.

3. Definitions

The UK General Data Protection Regulation (" UK GDPR") refers 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)

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

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

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

- "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 subjectsare students, employees and alumni or past students.

- "Personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, inparticular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes: name, address, email address, telephone number, date of birth, driver's license number, bank account number, credit or debit card numbers, dates of employment, academic performance and achievements, disciplinary record and

performance record.

- "Special categories of personal data" or "sensitive data" means personal data that is moresensitive and requires additional protection, including health or medical information, racialor ethnic origin, political opinions, religious or similar beliefs, trade union memberships, sexual life or orientation information, and genetic or biometric data.

4. Notification of Data Held

4.1. The University shall maintain a "Record of Processing" which records all the types ofpersonal data held and processed by the University, and the reasons for which it isprocessed. Thisrecord will be held by the Head of Governance.

4.2. The information which is currently processed by the University and the purposes forwhich it is processed are set out in a document entitled "Regent's University Processing of Personal Information". This document will be updated from time to timeand will be held by the Head of Governance.

5. Data protection by design and default

- Under the GDPR and the DPA, the University 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.

5.1 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. 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 after-thought.

5.2 Transfers of personal data outside the EEA

- Personal data can only be transferred out of the UK when there are safeguards in place to ensure an adequate level of protection for the data.

- Any transfer of personal data out with the EEA that uses the Standard Contractual Clauses (SCCs) as a safeguard will need to be evaluated and authorised by Head of Governance.

5.3 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 the University, 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). The University 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. Staff Responsibilities

6.1. All staff shall:

- Ensuring the processing of personal data in all formats is compatible with the data protection principles.

- Raising any concerns in respect of the processing of personal data with the DPO.

- Promptly passing 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 staff 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 the University in connection with their employment is accurate and up-to-date;

- Inform the University of any changes to information, for example, changesof address;

- Check the information which the University shall make available from timeto time, in written or automated form, and inform the University of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. The University shall not be held responsible for errors ofwhich it has not been informed; and

- Complete mandatory data protection training, as required.

6.2. When staff hold or process information about students, colleagues or other data subjects (for example, students' coursework, pastoral files, 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 and the Email Usage Policy.

- Staff shall ensure that all personal information is kept secure;
- Personal data is kept in accordance with the University's retention schedule;
- Reporting data security incidents, losses, near misses or unauthorised disclosures of personal data immediately to the attention of theGovernance Team and that they support the Governance Team 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 somecases.

6.3. When staff supervise students doing work which involves the processing ofpersonal information, they must ensure that those students are aware of theData Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate.

6.4. Staff 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 thatcontain 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 andprotected with passwords and encrypted with tools such as Bitlocker.
- Data on Portable storage devices must be encrypted and locked away when not in use.
- Confidential waste must be disposed of in accordance with the appropriateinternal procedures for confidential waste.

- Locking/logging off from PCs when away from the desk.

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

7. Student Responsibilities

7.1. All students shall:

- familiarise themselves with the Data Protection Agreement provided when theyregister with the University;
- ensure that all personal information which they provide to the University isaccurate and up-to-date;
- inform the University of any changes to that information, for example,changes of address; and check the information which the University shall make available from timeto time, in written or automated form, and inform the University of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. The University shall not be held responsible for errors ofwhich it has not been informed.

7.2. Students may process personal information (for example, in coursework or research). In those circumstances, they must comply with the requirements ofprocessing personal data and familiarise themselves with the document "DataProtection and Academic Research".

- All students shall successfully complete the required information compliance training before processing personal data for the purposes of their study.

8. Rights to Access Information

8.1. Staff, students and other data subjects in the University have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files.

8.2. Any person may exercise this right by submitting request preferably in writing to the Head of Governance (privacy@regents.ac.uk).

8.3. The University aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing by to Head of Governance (privacy@regents.ac.uk), to the person making the request.

8.4. The University will provide a copy of the information free of charge. However, should the request be considered excessive, repetitive or unfounded, we will charge a fee based on the administrative cost of providing the information.

8.5. Students are entitled to information about their marks for assessments.

9. Subject Consent

9.1. In some cases, the University is entitled to process personal data only with theconsent of the individual. If staff or students are in any doubt, then they should firstly check with the Head of Governance.

9.2. The indication of consent will be unambiguous and involve a clear affirmative action (an opt-in). It requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and is not a precondition of registering with the University.

9.3. Consent requests will be prominent, unbundled from other terms and conditions,concise and easy to understand, and user-friendly.

9.4. The University will maintain clear records to demonstrate consent.

9.5. Data subjects have the right to withdraw consent at any time by contacting the Head of Governance, email: privacy@regents.ac.uk.

10. Sensitive Information

10.1. The University may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin, or trade union membership. For example, some jobs or courses will bring the applicants into contact with youngpeople between the ages of 16 and 18, and the University has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job,and students for the courses offered. The University may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy, or for academic assessment.

10.2. The University may also ask for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The University will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency.

11. The Data Controller and Management Responsibility

11.1. Regent's University London Limited is the data controller under the Act.

11.2. The Board is ultimately responsible for compliance with the Act.

11.3. The Vice Chancellor's Executive Team (VCET) is responsible for the strategic implementation of the Data Protection Policy.

11.4. The Head of Governance is the University's Data Protection Officer and can offer advice on matters connected with data protection (privacy@regents.ac.uk) extension 7813. The Head of Governance reports to the Audit & Risk Committee on data protection compliance and any breaches of the Data Protection Act, and at least annually to the Board. The Head of Governance is responsible for updating the Data Protection Policy.

12. Retention of Data

12.1. The University will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements.

12.2. Personal information is retained for no longer than the periods permitted in the University's retention schedule.

12.3. Out of retention information will be destroyed securely, for example by shredding or appropriate electronic erasure. Please seek further advice from the Head of Governance extension 7813, email:privacy@regents.ac.uk

13. Compliance

13.1. Compliance with the Act and UK GDPR is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings.

13.2. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Head of Governance by telephone on extension 7813 or by e-mail at privacy@regents.ac.uk

13.3. Any individual, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated datacontroller initially. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

13.4. 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 the University's final response to your complaint. For further advice on making a complaint to the ICO, please see their website at www.ico.gov.uk

14. 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

15. Related Documents.

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

- IT Acceptable Use Policy
- IT Remote Access Policy
- Email Usage Policy
- Information Security Policy
- Data Protection Breach Notification Procedure
- Subject Access Request Procedure

16. Policy Review

- This policy will be reviewed at least annually and whenever there is a significant change to legislation.