Data Protection Policy

Office of the CIO

Version 1.7.

Document Revision History

Version	Date	Author	Description of Change
	Jan-17		
	Aug-17		
1.5.	Jan-18	Darren Tysoe - CIO	Changes incorporated under the General Data Protection Regulations (GDPR).
1.6.	Jan-18	Darren Tysoe - CIO	Amended to include 'Clean desk principles' (section 5.5)
1.7.	Apr-18	Darren Tysoe - CIO	Amended to replace governance email address with privacy

Contents

Data Protection Policy

1. Introduction

1.1. Regent's University London recognises its responsibilities with regard to the management of the requirements of the Data Protection Act 1998, and from 25 May 2018, the General Data Protection Regulation (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 1998, and from May 2018, 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 must comply with.

2. The Principles

2.1. 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 others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (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 aims to strengthen the rights of individuals. The individual data protection rights 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.

3. Definitions

The General Data Protection Regulation ("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

"Data controller", or "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 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, agency or 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 subjects are 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, in particular 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 more sensitive and requires additional protection, including health or medical information, racial or 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 of personal data held and processed by the University, and the reasons for which it is processed. This record will be held by the Governance office.

4.2. The information which is currently processed by the University and the purposes for which 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 time and will be held by the Governance Office.

5. Staff Responsibilities

5.1. All staff shall:

- 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, changes of address; and
- check the information which the University shall make available from time to 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 of which it has not been informed.

5.2. 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.

5.3. Staff shall ensure that:

- all personal information is kept securely;
- personal data is kept in accordance with the University's retention schedule;
- any data protection breaches are swiftly brought to the attention of the Governance Team and that they support the Governance Team 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.

5.4. When staff 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.

5.5. 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 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 and protected with passwords and encrypted with tools such as Bitlocker
- Data on Portable storage devices must be encrypted and locked away
- Confidential waste must be disposed of in accordance with the appropriate internal procedures for confidential waste
- Logging off from PCs when away from the desk

6. Student Responsibilities

6.1. All students shall:

- familiarise themselves with the Data Protection Agreement provided when they register with the University;
- ensure that all personal information which they provide to the University is accurate 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 time to 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 of which it has not been informed.

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

7. Rights to Access Information

7.1. 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.

7.2. Any person may exercise this right by submitting a request in writing to Company Secretary (privacy@regents.ac.uk).

7.3. 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 Company Secretary (privacy@regents.ac.uk), to the data subject making the request.

7.4. 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. Subject Consent

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

8.2. 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.

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

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

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

.

9. Sensitive Information

9.1. 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 young people 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.

9.2. 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.

10. The Data Controller and the Designated Data Controllers

10.1. Regent's University London is the data controller under the Act, and the Chief Information Officer and Director of Information Services is ultimately responsible for implementation.

10.2. Responsibility for day-to-day matters will be delegated to the Company Secretary, Directors, Deans and Heads of School as designated data controllers.

10.3. Information and advice about the holding and processing of personal information is available from the Company Secretary (privacy@regents.ac.uk) extension 7813.

11. Assessment Marks

11.1. Students shall be entitled to information about their marks for assessments, however this may take longer than other information to provide. This information may not be withheld.

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.

12.4. Please seek further advice from the Company Secretary extension 7813, email: privacy@regents.ac.uk

13. Compliance

13.1. Compliance with the Act and 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 Company Secretary 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 data controller initially. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

14. HESA Data Collections

Data about you will be supplied to HESA for the purposes set out below. All information is used in compliance with the Data Protection Act 1998, and from 25 May 2018 with the General Data Protection Regulation (GDPR). The full HESA Data Collection Notice is available from this link: http://www.hesa.ac.uk/fpn

Here is a summary.

14.1. HESA collects data about the personal characteristics of students and information about their studies and qualifications. This might include sensitive details about students' personal lives used for equality and diversity monitoring.

14.2. Purpose 1 – Named data used for public functions
Your HESA information is used by public authorities for their statutory and/or public functions including funding, regulation and policy-making purposes. Your information is provided by reference to your name, but your information will not be used to make decisions about you.

14.3. Purpose 2 - Administrative uses
Your named data may be processed by public authorities for the detection or prosecution of fraud. These uses of your HESA information may result in decisions being made about you.

14.4. Purpose 3 - HESA publications
HESA publishes statistics about students in higher education.

14.5. Purpose 4 - Equal opportunity, research, journalism and other processing for statistical and research purposes
HESA information is used for research into higher education and the student

population. This research can be academic, commercial, journalistic or for personal reasons. HESA prohibits the identification of individual students by those carrying out this research and information is not shared on a named basis.

14.6. Linking of your HESA information to other information
HESA information is sometimes linked to other data sources to enable more detailed research and analysis.

14.7. The HESA Initial Teacher Training record ("ITT")
Information about teacher training students in England is submitted to the National College of Teaching and Leadership via HESA.

14.8. Student and leaver surveys
You may be asked to provide information about your experience as a student and your activities after you graduate as part of national surveys.

14.9. Your rights
Data protection legislation gives you rights over your personal data. These include rights to know what information is processed about you and how it is processed. These rights have to be met by HESA and any other organisation which takes decisions about how or why your information is processed.

14.10. Data transfers to other countries
Your HESA information may be transferred to countries outside the European Union for the purposes described above.

15. Related Documents.

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

- IT Acceptable Use Policy
- IT Remote Access Policy
- Email Usage Policy