DATA PROTECTION POLICY

1. Introduction

This policy sets out how The Robert Gordon University shall comply with the requirements of the Data Protection Act 1998 and was created with reference to the JISC *Data Protection Code of Practice for the HE and FE sectors*, Version 2.0, 12 January 2001.

2. Purpose

The purpose of this policy is to ensure that the University, its staff, contractors and its students comply fully with the provisions of the Data Protection Act when processing personal data. Personal data is data which relates to an individual, and includes information that affects the person's privacy in personal or family life, or in a business or professional capacity.

The University is required to adhere to the eight principles of data protection as laid down by the Act. In accordance with those principles, this policy seeks to ensure that personal data shall be:

1. processed fairly and lawfully
2. processed for specified purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the data subject's rights
7. kept secure
8. not transferred outside the countries of the European Economic Area (EEA) without adequate protection.

3. Responsibilities

3.1 The University

The University recognises its responsibility under the Act as a data controller.

On behalf of the University, the **Director of Planning and Policy Development** has overall executive responsibility for the Act's compliance and is supported in this function by the University's Data Protection Officer.

Monitoring of the implementation of this policy is undertaken, on an annual basis, by the University's, Executive.

The University will provide a range of Data Protection awareness training to support staff in their roles and responsibilities and to students as required in the course of their studies.

3.2 The Data Protection Officer

The Data Protection Officer is responsible for;

- providing advice, guidance and training on data protection responsibilities and compliance with this policy;
- administering subject access requests;
- liaising with the Information Commissioner's Office (ICO);
- preparing and submitting the University's reporting requirements, including the annual data protection notification;
- co-ordinating the development and delivery of training materials;
- recording any incidences of breach of this policy.

3.3 Staff

All staff must;

- adhere to the terms of this policy;
- ensure that all personal information entrusted to them is kept securely;
- ensure no personal information is disclosed to any unauthorised third party;
- ensure that their own personal data held by the University is kept up to date.

Where members of staff are responsible for supervising students carrying out work which involves the processing of personal information (for example in research projects or on placements), staff must ensure that students are given appropriate guidance to ensure that they comply with this policy, and are aware that failure to adhere to that guidance could lead to action being taken against the student.

3.4 Heads of Schools and Departments

In addition, Heads of Schools and Departments must;

- ensure that their respective Schools and Departments fully comply with this policy;
- actively promote compliance to their staff;
- ensure that adequate procedures are in place for the back-up, storage and destruction, when appropriate, of personal data;
- inform the Data Protection Officer of any changes to the processing/collection of personal information that would affect the University's notification to the ICO.

In carrying out these responsibilities, the Head of School or Department may identify a senior member of staff to act as a Data Protection Co-coordinator, who will be a knowledgeable and accessible point of contact for people within the School/Department who have questions about data protection issues.

3.5 Contractors

The University is responsible for the use made of personal data by anyone working on its behalf. Heads of Departments/Schools, who employ contractors, must ensure that such contractors;

- adhere to the terms of this policy;
- do not have access to personal data beyond that required for the work to be carried out;
- return or destroy personal data on completion of the work.

3.6 Students

Students must adhere to this policy where relevant and as instructed by staff (refer to 3.3 above).

3.7 Researchers

Researchers must ensure that they seek, and gain explicit consent from research participants for any data sharing purposes including; proposed open access publication and any open data opportunities that may arise in the future. **Please refer to the Research Ethics and Research Governance policies**

4. Notification to the Information Commissioner's Office.

In compliance with the Act, the University will annually notify the Information Commissioner's Office (ICO) of its personal data processing activities.

The University's current notification can be viewed on the website of the ICO (www.ico.gov.uk).

Staff and students must only process personal data for the purposes listed within the University's current notification. Processing undertaken outside of the University's notification is unlawful.

5. Data Security

The University, and its staff and students individually, are responsible for ensuring personal data is securely held. Staff and students must ensure that they employ safeguards for personal data proportional to the risks presented in its use. University staff and students must not take personal data off-campus unless absolutely necessary, and only then with the permission of their Head of School/ Department. Staff and students who must take personal data off-campus must ensure that the data is secure. Please refer to the Mobile Computing Policy for further information.

All Research data collected by researchers must be held securely.

5.1 Clear Desk / Clear Screen

Staff must minimise the amount of personal data and commercially sensitive information in their workspace at all times. At the end of the working day, or when leaving the office for a significant period of time, staff are expected to tidy their workspace of papers, 'Post it' notes, Business cards and any removable media containing personal or commercially sensitive data. The University will provide an under desk locker and/or lockable cupboards for this purpose these should be kept locked when unattended for an extended period.

Particular care must always be taken to protect Personal data from 'third party' (e.g. maintenance engineers, members of the public, contractors etc.) visitors to places of work who are not authorised to read/view personal data or commercially sensitive information.

Workstations (computers, tablets etc.) must be secured when unattended to prevent unauthorised access, and logged off at the end of the working day. Ensure that sensitive information cannot be read by others.

Managers/supervisors should be aware who has access to keys to offices particularly during hours when authorised staff aren't working in them, and should ensure that relevant information cannot be viewed by any unauthorised staff.

6. Electronic Storage and Transmission

The use of IT to store and process personal data can provide very effective access control, protection and security if properly implemented. It can, however, also allow personal data to be exposed – potentially at quite a significant scale, if the necessary controls and safeguards are not in place or are not followed.

Personal data held in electronic format should normally be stored on and processed through the University's enterprise-wide IT systems or held on the S: and H: drives. It should not be stored on laptops, portable electronic media or mobile devices other than exceptionally on a temporary basis, and then only if held in an encrypted format. Refer to the policy " Mobile Computing: Information Security for Sensitive Information".

Unrestricted internet publishing of personal data makes that personal data available outside of the EEA in contravention of the Act.

Such publishing is only permissible where:

- the data subject has given written consent.
- the personal data is already publicly available in another form. In this case it is best practice to inform the data subject of the intention to web publish.

7. Transfer of Data

Personal data must not be disclosed to any third party, or outside the EEA, without consultation with the Data Protection Officer. The University has legal and statutory responsibility to disclose personal data to certain third parties. Details of these bodies can be found on the Data Protection web pages under, 'Transferring personal data from RGU to other organsations'.

Research data shared with collaborators by digital means should be done securely using a service based in the EU as required by Principle 8 of the Data Protection Act, and other applicable legislation.

8. References

Guidance for staff regarding the provision of references and the release of references provided by third parties is available on the Data Protection web pages at

https://you.rgu.ac.uk/org/ig/dp/SitePages/Reference_Requests.aspx

9. Subject Access Requests

Individuals may request access to their own personal data held by the University via a Subject Access Request. Any individual wishing to exercise this right should do so in writing to the Data Protection Officer. Further information is available from the Data Protection Officer or on the University's Data Protection web pages.

10. University Use of Personal Data

The University holds and uses personal data relating to its staff and students in accordance with *Data protection (Employee Records)*, and *Prospective and Current Students Data Protection Statement* available on the Data Protection web pages.

The University recognises that under the Act an individual can request that their own personal data is not processed for one or more purposes.

The University may decline such a request. Individuals should be aware that in exercising this right they may disadvantage themselves or, in extreme cases, may be unable to begin/continue their studies or employment with the University.

11. Retention and Disposal of Records

Data must only be retained for as long as required in connection with the specific purpose collected.

Staff and students must consult the University's *Master Retention Schedule* for guidance regarding disposal of data.

12. Security Breach

12.1 Any breach of the Data Protection Act or the requirements of this Policy should be immediately reported to the Data Protection Officer for action.

12.2 A report of a significant suspected breach of the Act will be dealt with as follows;

- the Data Protection Officer will take steps to attempt to contain and recover the personal information where possible.

- the Data Protection Officer shall report to the Director of Planning & Policy Development on the nature of the breach, the risks of re-occurrence and impact upon University operations.

- The Director will, in consultation with the Data Protection Officer, assess whether it is necessary to notify either those individuals affected or the relevant Regulatory Authorities about the breach and will also decide, after consultation with senior members of staff, whether to convene a Breach Investigation Panel.

  Such a Panel may consist of, amongst others;

- Director of Planning and Policy Development (Chair)
- University Solicitor
- Data Protection Officer
- Head of Human Resources

12.3 The Panel will consider;

- whether a breach has occurred
- how that breach arose
- what action, if any should be taken to avoid future occurrences
- whether any action should be recommended against any member of staff or student
- the effectiveness of the University's response to the breach

Where the potential breach involves the Director of Planning and Policy's area of responsibility, their role in this context shall be undertaken by the Principal or nominee.

12.4 On completion of their investigation the Chair of the Panel shall submit a full report to the Executive.

13. Complaints

Any issues regarding the operation of this policy should be made in the first instance to the Data Protection Officer. The communication will be acknowledged and a detailed reply will be issued within 21 days where possible.

Where the complainant remains dissatisfied, the matter shall be referred to the Director of Planning & Policy Development, and may be dealt with in accordance with the University's Complaints procedure.

Where the matter cannot be resolved to the satisfaction of the complainant, it may be referred to the ICO.

Refresh 10
March 2016