Information Governance Policy

Approved by	The Executive		
Date approved	March 2018	**Status**	Approved
Policy owner	Director of Planning & Policy Development	**Impact assessed**	Yes
Version	V1	**Date of next review**	March 2021

1. Policy Statement & Scope

1.1 The Robert Gordon University is fully committed to being a transparent organisation which fully complies with information governance legislation including:

1.1.1 The General Data Protection Regulations (2018) (GDPR)

1.1.2 The Freedom of Information (Scotland) Act 2002 (FOISA)

1.1.3 The Environmental Information (Scotland) Regulations 2004 (EIR)

1.2 The purpose of this policy is to provide a single framework to outline the responsibilities of the University and the ways in which it will achieve a robust system of good information governance.

1.3 This policy is inclusive of to all recorded information, both electronic and hard copy, held by the University including (although not exclusively): minutes, correspondence, policies, hand-written notes, calendar, diaries, expense forms, research material, contracts and procurement documentation.

1.4 This policy is supplemented by a number of other documents and procedures. This includes the University publication scheme[1], the Master Records Retention Schedule[2] and procedural guidance for data protection, freedom of information and records management.

2. Data Protection

2.1 The Robert Gordon University recognises the importance of the principles of data protection and seeks to fully comply with the provisions of the GDPR. The University is registered with the Information Commissioner's Office (ICO) and processes personal data including employment records, student records, alumni records and research projects among others.

2.2 Personal data is defined as data which relates to an identifiable individual and includes information that affects the person's privacy in personal or family life, or in a business or professional capacity.

2.3 The University will also process a certain amount of special category data. This is defined as data that reveals:

2.3.1 Racial or ethnic origin;

[1] http://www.rgu.ac.uk/file/university-publication-scheme-pdf-527kb
[2] https://you.rgu.ac.uk/org/ig/Pages/MasterRetentionScedule.aspx

2.3.2 Political opinions;

2.3.3 Religious or philosophical beliefs;

2.3.4 Trade union membership;

2.3.5 Genetic and biometric data;

2.3.6 Health;

2.3.7 Sex life or sexual orientation.

2.4 In processing personal data the University is required to adhere to the seven principles of data protection laid out in the GDPR. Personal data must be:

2.4.1 Processed lawfully, fairly and in a transparent manner.

2.4.2 Collected and processed for specified, explicit and legitimate purposes.

2.4.3 Adequate, relevant and limited to what is necessary for processing purposes.

2.4.4 Accurate and up to date.

2.4.5 Kept in a form which permits ID of data subjects for no longer than is necessary

2.4.6 Protected against unauthorised or unlawful processing, accidental loss or destruction or damage

2.4.7 The University also has a requirement to demonstrate compliance with these principles.

2.5 In order to comply with the requirements of processing personal data, the University will publish privacy statements to ensure individuals understand how their data is being processed.

2.6 The University will undertake Data Protection Impact Assessments when processing of data has a risk to the rights and freedoms of individuals.

2.7 Individuals have a number of rights under the GDPR which must be adhered to by the University in processing personal data. These include:

2.7.1 The right to be informed.

2.7.2 The right of access.

2.7.3 The right to rectification.

2.7.4 The right to erasure.

2.7.5 The right to restrict processing.

2.7.6 The right to data portability.

2.7.7 The right to object.

2.7.8 Rights in relation to automated decision making and profiling.

2.8 Individuals are entitled to make a subject access request to the University to obtain confirmation that their data is being processed, access to their personal data and other supplementary information. The University will provide this information free of charge, unless a request is found to be manifestly unfounded or excessive, and will always seek to provide the information without delay and within the one month period.

2.9 While the University will always seek to fully comply with the requirements of the GDPR, there are procedures in place in case of a data protection breach. The University will inform the ICO and the individuals involved where required and an investigation will be carried out by the Data Protection Officer.

3. Freedom of Information

3.1 The Robert Gordon University is committed to a culture of openness of information and transparency and seeks to comply fully with the obligations of the Freedom of Information Scotland Act and the Environmental Information Regulations.

3.2 The key statutory obligations that the University has in relation to this are as below:

3.2.1 Publishing and maintaining a publication scheme as well as publishing and maintaining publication schemes for all wholly-owned active and dormant companies. The University has adopted the Model Publication Scheme which includes different categories of information which is published on the

website. The University will seek to make all published information easily available online.

3.2.2 Disclosure of request information held by the University, subject to exemptions under FOISA. The University will seek to respond to information requests as soon as possible and always within the 20 working day statutory limit.

3.2.3 Proactively making environmental information available;

3.3 Monitoring of compliance in meeting the 20 working day statutory limit, number of reviews request, review decisions, fees charged and exemptions applied will be carried out.

4. Records Management

4.1 Records are defined as "information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business." Records management is defined as managing records from their creation to destruction.

4.2 The University recognises the importance of efficient records management in supporting our core functions and compliance with legal and statutory obligations. As such the university will maintain its own records in accordance with the Scottish Government's Section 61 Code of Practice on Records Management.

4.3 The University aims to ensure that all records are:

4.3.1 Authentic – they are what they say they are

4.3.2 Reliable – they can be trusted as a full and accurate record

4.3.3 Integrity – they have not been altered since they were created or filed;

4.3.4. Useable – They can be retrieved, read and used.

4.4 A proportion of the University's records, identified as having permanent administrative or historic value, will be selected for permanent retention and held within the University's Archives. These will serve as an enduring record of the University's development, conduct of business and achievements and as a resource for research.

4.5 The University has an obligation, under section 61 of FOISA to establish practices in relation to the 'keeping, management and destruction' of records. The University has a master retention schedule (MaRS) which is based on the Joint Information Systems Committee (JISC) retention schedule. The MaRS is used as the basis for informing retention decisions and must be adhered to by all staff creating, managing and destroying records.

5. Roles & Responsibilities

5.1 The Executive

5.1.1 The Executive is responsible for complying with the legislative requirements of GDPR and FOISA and ensuring that all staff have an understanding of the requirements of each of the strands of good information governance. Further, the Executive has a responsibility to ensure that all staff who have individual responsibilities in terms of information governance have undertaken appropriate, ongoing training.

5.1.2 The University is the owner of all records created or received by University staff. The Executive has a responsibility to ensure robust records management procedures are embedded within the organisation, to consider the role of records management in risk management and to provide clear guidance and training to staff to ensure they are able to comply fully with the requirements of records management.

5.2 Strategic Responsibility

5.2.1 The Director of Planning and Policy Development has overall strategic responsibility for Information Governance and is the designated Data Controller for the University. The Director of Planning & Policy Development will oversee compliance and work towards creating a transparent culture and ensure effective implementation and review of Information Governance policy and procedures.

5.3 Operational Responsibility

5.3.1 The Information Governance & Complaints Officer has operational responsibility for the effective day-to-day management of the University's Information Governance framework and is the designated Data Protection Officer for the University. The responsibilities of the this role include:

- Providing advice, guidance and training on data protection, freedom of information and records management responsibilities;
- Administering Freedom of Information & Environmental Information Regulation requests and assisting the Information Governance Champions positioned across the University;
- Administering subject access requests;
- Liaising with the Information Commissioner's Office (ICO)
- Administration of the University Archives for records retention;
- Recording any incidences of breach of this policy and investigating as necessary.

5.4 Head of School/Department

Heads of Schools and Departments must:

- Actively promote compliance to their staff and ensure that they fully comply with this policy
- Ensure staff have access to training and resources in order to meet compliance obligations
- Appoint departmental Information Governance Champions

5.5 Staff

5.5.1 Each member of staff has individual responsibilities in order to assist the University in delivering good information governance and in ensuring compliance with the relevant legislation. Staff must:

- Adhere to the terms of this policy and associated guidance;
- Familiarise themselves with the individual information governance procedures;
- Process personal data in accordance with the GDPR principles;
- Ensure that 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;
- Follow records management procedures to ensure that records are created, managed and destroyed appropriately, in line with University procedures.
- Have an awareness of retention periods for any records they are creating or processing.
- Undertake training as required.
- Report any data protection breaches to the Data Protection Officer and their Head of School/Department.

5.5.2 Where members of staff are responsible for supervising students carrying out work which involves the processing of personal information held by the University, 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.

5.6 Information Governance Champions

There should be an appointed champion in each School and Department. This individual should:

- Act as the first point of contact for colleagues within department regarding queries on freedom of information requests, subject access requests and records management queries.
- Act as the single point of contact for the information governance officer in dealing with any information governance queries.
- Undertake training as required.
- Ensure department is complying with the master retention schedule and keeping it up to date.

5.7 Students

5.7.1 Where appropriate, such as when undertaking research or professional practice, students should ensure they are aware of this policy and fully comply with it, as instructed by staff.

6. Review

This policy will be reviewed on an annual basis or as legislation changes requirements.