ROBERT GORDON UNIVERSITY ABERDEEN

Information Governance Policy

Approved by	The Executive		
Date Approved	October 2022	**Status**	Approved
Policy Owner	University Secretary and VP Corporate Operations	**Impact assessed**	Yes
Version	2	**Date of next review**	October 2025

Version Number	Purpose/Change	Date
1	Creation of policy	March 2018
2	The Policy has been updated into the new standard template to comply with accessibility regulations, to reflect job title and policy name changes and to include links to related documents. References to EU legislation have been updated to UK legislation following the exit of the UK from the EU. Several explanations and definitions have been added to provide further guidance for data protection matters and to demonstrate compliance with relevant regulations. FOI and EIR operations have also been expanded on to better demonstrate the role of the Information Governance team.	October 2022

INFORMATION GOVERNANCE

1. Policy Statement & Scope

1.1 As a public body Robert Gordon University is governed by the following legislation:

1.1.1 The Data Protection Act (2018) and the UK General Data Protection Regulations (UK 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 legal responsibilities of the University and the ways in which it will achieve a robust system of good information governance. The failure to meet these obligations may result in the breach of law.

1.3 This policy is inclusive of all recorded University information (both electronic and hard copy) including records held on university and personal devices, the following list of examples are not exclusive: emails, social media communications such as WhatsApp messages, meeting minutes, correspondence, policies, hand-written notes, calendars, diaries, expense forms, research material, contracts, and procurement documentation.

1.4 This policy is supplemented by several other documents and procedures. This includes the University Publication Scheme, the Master Records Retention Schedule and procedural guidance for data protection, freedom of information and records management.

2. Data Protection

2.1 Robert Gordon University recognises the importance of the principles of data protection and seeks to fully comply with the provisions of the UK 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 As detailed under UK GDPR, the University has a designated Data Protection Officer, the Policy and Information Governance Manager, details of whom can be found on the University's Data Protection website.

2.3 Personal data is defined as data which relates to an identifiable individual and is about them, this wide ranging and would include information that affects the person's privacy in personal or family life, or in a business or professional capacity. A person to whom persona data relates is known as the Data Subject.

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

2.4.1 Racial or ethnic origin;

2.4.2 Political opinions;

2.4.3 Religious or philosophical beliefs;

2.4.4 Trade union membership;

2.4.5 Genetic and biometric data;

2.4.6 Health;

2.4.7 Sex life or sexual orientation.

2.5 The processing of personal data is when it is used in activities such as; reading, storing, using, collecting, transferring/sharing, altering, destroying, or disclosing.

2.6 In processing personal and special category data, the University is required to adhere to the seven principles of data protection laid out in the UK GDPR. Personal data must be:

2.6.1 Processed lawfully, fairly and in a transparent manner.

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

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

2.6.4 Accurate and up to date.

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

2.6.6 Protected against unauthorised or unlawful processing, accidental loss or destruction or damage.

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

2.7 The University will only collect, process, and share personal data when there is a legal purpose. The UK GDPR sets out these purposes, in Article 6, and are listed below:

2.7.1 Consent of the data subject;

2.7.2 Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;

2.7.3 Processing is necessary for compliance with a legal obligation;

2.7.4 Processing is necessary to protect the vital interests of a data subject or another person;

2.7.5 Processing is necessary to perform tasks in the public interest;

2.7.6 Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

2.8 When processing special category data, the University will ensure the purpose meets one of the legal purposes in Section 2.7 and one additional basis set out in Article 9 of UK GDPR:

2.8.1 Explicit consent (except where applicable law advises otherwise);

2.8.2 Necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;

2.8.3 Necessary in the vital interests of the data subject or another individual;

2.8.4 Necessary for legitimate activities by a not-for-profit organisation;

2.8.5 Relates to personal data made public by the data subject;

2.8.6 Necessary for the establishment, exercise or defence of legal claims;

2.8.7 Necessary for reasons of substantial public interest;

2.8.8 Necessary for the purposes of health or social care;

2.8.9 Necessary for reasons of substantial public interest in the area of public health;

2.8.10 Necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

2.9 Where the University processes criminal conviction data, the University will ensure the purpose meets one of the legal purposes in Article 6 of GDPR (see section 2.7 above) and meets a condition from Schedule 1 of the Data Protection Act 2018.

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

2.11 The University will undertake Data Protection Impact Assessments when processing of data has a high risk to the rights and freedoms of individuals including but not limited to activities involving vulnerable people, special category data, automated processing and decision-making (including profiling).

2.12 Personal data will only be collected for specified legal purposes; it should not be processed for different purposes than those disclosed when first collected.

2.13 When required, the University will share personal data with third parties (individuals or organisations out with the University) and vice versa. A written agreement must be in place before personal data is shared either with or by the University. This agreement must contain who is the Data Controller as explained below:

2.13.1 The University will, in most situations, act as Data Controller when processing personal data and ensure if the services of a Data Processor, are engaged, the processor has sufficient guarantees about their data security and protection in place before personal data is shared. This must be in the form of a contract with specific data protection clauses. There must also be a secure method for transferring the data.

2.13.2 The University will on occasion, act as the Data Processor for a third party acting as Data Controller. Staff should ensure that the Data Controller's instructions are legal before agreeing and once done, the University must only act within those instructions of the Data Controller.

2.13.3 Alternatively, a Data Sharing Arrangement may be in place, where the University and the third party both act as Data Controller. The agreement should contain the purpose of the arrangement, the data to be shared, the lawful basis and operational procedure for sharing data.

2.14 UK GDPR restricts the transferring of personal data to the UK or the European Economic Area (EEA) unless appropriate safeguards are in place. A transfer of personal data can include the sending, viewing, or accessing of data originating in one country to a different country. Guidance should be sought from the Data Protection Officer before agreeing to or transferring data internationally, as an international data transfer agreement (IDTA) and risk assessment may be required to be in place.

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

2.15.1 The right to be informed;

2.15.2 The right of access;

2.15.3 The right to rectification;

2.15.4 The right to erasure;

2.15.5 The right to restrict processing;

2.15.6 The right to data portability;

2.15.7 The right to object;

2.15.8 Rights in relation to automated decision making and profiling.

2.16 Under the right of access, individuals are entitled to make a Subject Access Request (SAR) to the University to obtain confirmation of how 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. SAR's should be sent to the Data Protection Officer at dp@rgu.ac.uk.

2.17 As part of the University's commitment to data protection all University staff receive mandatory data protection training as part of the onboarding process along with periodic refresher training.

2.18 The University has designated Information Governance Champions within each school and department, these individuals are the point of contact and provide basic data protection advice.

2.19 While the University will always seek to fully comply with the requirements of the data protection legislation, there are procedures in place in case of a personal data breach. Data breaches **must** be immediately reported to the relevant Information Governance Champion who in turn will notify the Data Protection Officer. The University has a legal obligation to inform the ICO and the individuals involved in certain circumstances which must be done within 72 hours. In all cases an investigation will be carried out by the Data Protection Officer. A record of data breaches, causes, effects and remedial actions will be kept by the Data Protection Officer.

3. Freedom of Information and Environmental Information

3.1 Robert Gordon University is defined as a public authority for the purposes of Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information Regulations 2004 (EIR) and therefore must comply with the above legislation. The Scottish Information Commissioner can impose sanctions and instruct the release of information.

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 for the University as well as 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 made available on the website. The University will seek to make all published information easily available online.

3.2.2 Disclosure of requested information held by the University;

3.2.2.1 Freedom of Information (FOI) requests and Environmental Information (EI) requests are answered by the Information Governance team, staff in other departments/schools should recognise such requests and send on to the Information Governance team to process and to record relevant data.

3.2.2.2 The University will receive many "business as usual" requests such as prospective students asking for information on courses or requesting prospectuses. These requests will be handled by the relevant department or school and do not need to be recorded.

3.2.2.3 Under specific circumstances the information requested can be subject to exemptions under FOISA and EIR. The Information Governance team will assess and apply such exemptions when appropriate.

3.2.2.4 The Information Governance team **must** respond to information requests as soon as possible and always within the 20-working day statutory limit.

3.2.3 Proactively make environmental information available;

3.2.4 Monitor and report on FOI and EIR statistics to the Scottish Information Commissioner including meeting the 20-working day statutory limit, number of reviews requested, review decisions, fees charged, and exemptions applied.

3.3 Information on how to submit an FOI or EI request can be found on the University's website.

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 Genuine – 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 UK GDPR, FOISA, EIR and ensuring that all staff understand 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 can comply fully with the requirements of records management.

5.2 Strategic Responsibility

5.2.1 The University Secretary has overall strategic responsibility for Information Governance and is the designated Data Controller for the University. The University Secretary 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 Policy and Information Governance Manager as the University's Data Protection 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 this role include:

5.3.1.1 Providing advice, guidance and training on data protection, freedom of information and records management responsibilities;

5.3.1.2 Administering Freedom of Information & Environmental Information Regulation requests and assisting the Information Governance Champions positioned across the University;

5.3.1.3 Administering subject access requests;

5.3.1.4 Liaising with the Information Commissioner's Office (ICO);

5.3.1.5 Administration of the University Archives for records retention;

5.3.1.6 Recording any incidences of breach of this policy and investigating as necessary.

5.4 Dean of School and Heads of Department

5.4.1 Deans of Schools and Heads of Departments must:

5.4.1.1 Actively promote compliance to their staff and ensure that they fully comply with this policy;

5.4.1.2 Ensure staff have access to training and resources in order to meet compliance obligations.

5.4.1.3 Appoint 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:

5.5.1.1 Adhere to the terms of this policy and associated guidance;

5.5.1.2 Familiarise themselves with the individual information governance procedures;

5.5.1.3 Process personal data in accordance with the UK GDPR principles;

5.5.1.4 Ensure that their own personal data held by the University is kept up to date;

5.5.1.5 Follow records management procedures to ensure that records are created, managed and destroyed appropriately, in line with university procedures;

5.5.1.6 Have an awareness of retention periods for any records they are creating or processing;

5.5.1.7 Undertake training as required;

5.5.1.8 Report any data protection breaches to the Data Protection Officer and their Head of School/Department.

5.5.1.9 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 may lead to action being taken against the student.

5.6 Information Governance Champions

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

5.6.1.1 Act as the first point of contact for colleagues within department regarding queries on freedom of information requests, data protection queries and records management queries;

5.6.1.2 Act as the single point of contact for the information governance officer in dealing with any information governance queries;

5.6.1.3 Undertake training as required;

5.6.1.4 Ensure department is complying with good record management principles including 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. Compliance

6.1 Staff should be aware that failure to comply with the Information Governance policy, dependent on the severity, may result in disciplinary actions and if found to have breached the legislation stated in the policy, in legal proceedings.

7. Review

7.1 This policy will be reviewed every three years or as legislation changes require.

ROBERT GORDON
UNIVERSITY ABERDEEN

Robert Gordon University,

Garthdee Rd,

Aberdeen AB10 7AQ