Information Governance Framework

THE UNIVERSITY of EDINBURGH

Summary

The Information Governance Framework describes the arrangements the University has in place to ensure key business information is handled legally, securely, efficiently, and effectively.

Scope: Overarching approach to information governance

This Framework applies to anyone, acting on behalf of the University, who processes University information. While individual information governance activities or policies may be undertaken by or apply to specified groups, the overarching Framework must be referred to by all.

Contact	Governance and Strategic Planning	Info.Governance@ed.ac.uk
Framework Sponsor	Vice-Principal and University Secretary	

Document control

Dates	**Version approved**: 24.02.26	**Effective date:** 21.01.25	**Equality impact assessment:** Not required for Framework	**Last Reviewed:** 24.02.26	**Next Review:** No later than February 2029

Approving authority	University Executive
Related policies	All policies listed on page 13 of the Information Governance Framework.
Alternative format	If you require this document in an alternative format please email Info.Governance@ed.ac.uk.
Keywords	Information governance, collections management, computing acceptable use, data protection, digital perseveration, information security, records management, research data, research ethics, risk management

Information Governance Framework

THE UNIVERSITY of EDINBURGH

1. Introduction

The University generates, uses, shares, and stores a vast array and quantity of information. Every day, in every corner of the University, staff and students rely on information to develop knowledge, solve problems, appraise options, make decisions, plan (both for the immediate and long term) and take appropriate action.

It is therefore critical that the University has effective arrangements in place to safeguard this key asset and which give assurance that it is complying with the legal, regulatory, and moral responsibilities that accompany the handling of information. Collectively such arrangements are referred to as “information governance”.

Effective information governance ensures policies, procedures, structures, systems, controls, reporting mechanisms and people (with clear roles and responsibilities, and appropriate training) are in place to maximise the accuracy, integrity, value, and security of the information held by an organisation and that information risk is assessed and effectively managed.

2. Purpose

This Framework sets out the University’s overarching approach to information governance. Further detail regarding information governance activities and services, policies and procedures, roles and responsibilities, training and support and risk management can be found on the University’s website – to which links are provided.

3. Scope

Information governance spans how information is created, stored, used, shared, archived, and disposed of.

It covers the activities of information security, data protection, information and records management, risk management and legal and regulatory compliance.

It includes all University information, in any format including, but not limited to:

- paper, digital files (e.g. databases, Word documents, spreadsheets, webpages, email attachments), images, video footage, and metadata, i.e. information about data.
- electronic messaging (e.g. emails, WhatsApp, Microsoft Teams messages) and social media content (e.g. Facebook, LinkedIn), and
- information generated by artificial intelligence systems.

This Framework applies to anyone, acting on behalf of the University, who processes University information. While individual information governance activities or policies may be undertaken by or apply to specified groups, the overarching Framework must be referred to by all.

4. Definitions

For this Framework, the University deems the terms used to have the following meaning:

Data: raw, unanalysed facts/statistics.

Information: data that have been analysed, interpreted and organised/formatted to provide context and meaning.

Information asset: a single piece or collected body of information of value to its owner, which if inaccurate, lost or misused would adversely impact operational activity and decision-making and would be difficult and/or costly to replace.

Records: data or information (in any format) created, received or maintained by the University (or someone working or acting on its behalf) in the transaction of University business or conduct of University affairs and kept as evidence of those activities for business or accountability purposes.

Archived records: records, in any format, that have historical significance and have been selected for long-term preservation.

Research data: information (in any format) that is collected, observed, created or reused to produce, validate and enrich research findings and conclusions.

Research ethics: the application of ethical principles throughout the lifecycle of a research project, including the handling of research data and records.

Golden Copy: the authoritative, single source of a type of data, or official, master version of a record.

Retention Schedule: a schedule setting out why and for how long the University needs to keep specific categories of records, the event that triggers the start of the retention period and what happens to the records at the end of the retention period.

5. Principles

The following principles underpin the University's approach to information governance.

Accountability: roles and responsibilities are clearly defined. Everyone is aware of their responsibilities.

Transparency: there are clear processes describing information activities. There are records of processing activity.

Compliance: data protection legislation, freedom of information and other legislation, third-party data provider requirements and University policies are adhered to.

Protection: measures are in place to help maintain the integrity of information and safeguard information from loss, unauthorised access, alteration or disposal.

Availability: information is made available to the appropriate person when needed without compromising privacy or security.

Quality: information quality is a priority. Information is accurate, complete, consistent, timely, unique, and valid.

Lifecycle: the full information lifecycle is accounted for, from creation to disposal.

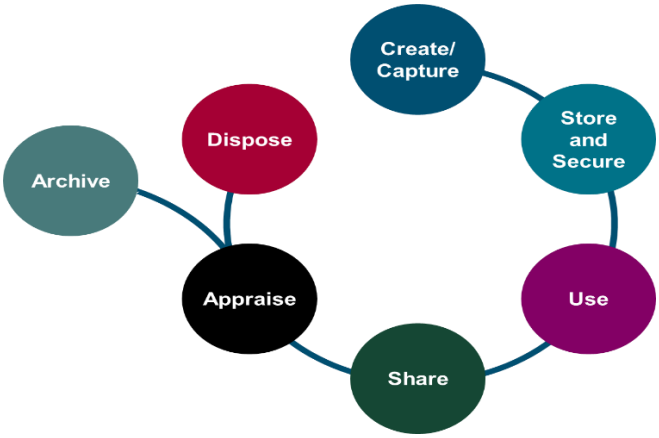

Figure 1. The information lifecycle

6. Information Governance Framework

The Framework pulls together and describes the:

a) overarching governance and management arrangements the University has in place to ensure the Framework is effective and fit for purpose;

b) key policies and standards which ensure the University fulfils its legal obligations;

c) individual, but inter-related and inter-connected, activities and services which support the information lifecycle;

d) underpinning training that is available to staff to ensure they are aware of and understand their responsibilities when requesting, receiving, creating, using, storing and disposing of University information; and

e) underpinning, and cross-cutting arrangements in place to report and manage information-related risks.

These arrangements are described in more detail below and depicted in Figure 2.

Information Governance Framework

Figure 2. University of Edinburgh Information Governance Framework

6.1 Accountability and Oversight

At University level, an **Information Governance Group**, comprised of senior members from each College, Professional Services Group, Information Compliance Services and Information Security, is in place to:

a) provide oversight of, and drive continuous improvement in, the University's arrangements for information governance; ensuring people, policies, procedures, systems, controls, and reporting mechanisms are in place to maximise the accuracy, integrity, value, and security of the information processed across the University; and to evaluate and address risks to this valuable University asset; and

b) provide assurance to the Risk Management Committee on the effectiveness of these arrangements.

Each member of the Group works with their respective Head of College/Professional Services Group to promote understanding of the Framework within their College/ Professional Services Group. Each College and Professional Services Group has reporting mechanisms in place to ensure their Schools and Departments are adhering to each part of the framework.

The Group's full terms of reference and membership can be found here.

The **Risk Management Committee:** reports to the Audit and Risk Committee, a Standing Committee of the University Court. The Risk Management Committee's full terms of reference and membership can be found here.

The **Audit and Risk Committee:** reviews the effectiveness of the University's corporate governance arrangements and risk management arrangements and provides assurances to Court on these areas. The Audit and Risk Committee's full terms of reference and membership can be found here.

University Executive: agrees all pan-University policies, including those related to information governance. It is responsible for implementing University Court's risk management policy, including considering updates on strategic level risks across the University, and ensuring corporate risks, e.g. to core information assets, are properly managed.

The University Executive's remit and membership can be found here.

University Court: the University's governing body and legal persona. This is the ultimate authority of the administration and management of the University. More information can be found here.

6.2 Information Security and Data Management

The Information Security team owns the University's information security risk strategy, policy and standards, and leads on information security initiatives. Alongside the Cyber Security Operations team, they provide advice on existing and emerging threats and deliver security awareness training.

Information Security Champions in Schools and Professional Services Departments help promote good information security practices and respond to local issues. Staff who volunteer for this role are provided with training and support by the Information Security team.

For each type of University data, e.g. employee, finance, student data, there is one University IT system that holds the golden or reference copy. Each Golden Copy has a Data Steward, responsible for looking after that data and reviewing requests for access to it.

All staff and students, and any other person with authorised access to University information or digital services and networks must comply with the University's Computing Acceptable Use Policy, the Information Security Policy and all Information Security Standards that apply to their work.

The activities in this pillar contribute to ensuring the University complies with data protection legislation.

6.3 Data Protection and Information Compliance

The activities of Data Protection help ensure the University meets its legal obligations regarding privacy and data protection.

The University's Data Protection Officer advises on and monitors the University's compliance with data protection legislation.

Data Protection Champions are in place in each School and Professional Services Department to support the Data Protection Officer to maintain compliance throughout the University.

The services provided by Information Compliance help ensure the University complies with freedom of information (FOI) legislation and environmental information regulations and subject access rights (SAR) under data protection legislation.

Information Practitioners are in place in each School and Professional Services Department to carry out FOI procedures and SAR requests. Staff in this role are provided with additional training and support by Information Compliance Services. However, all staff have a responsibility to comply with freedom of information and subject access request requirements.

All staff members, students and visitors must comply with the Data Protection Policy.

6.4 Records Management and Archive Management

Records Management ensures the University knows what information it has, where it is kept and how long to keep it. It helps ensure that records retain their essential characteristics throughout their lifespan, i.e. availability, integrity and confidentiality.

It comprises the Records Management Policy Framework and guidance on the creating, organising and disposing of a University record and on creating and reviewing retention schedules.

The Records Manager provides specialist records management advice and expertise to University staff and works closely with the University's Archivist on the selection and transfer of records to the University Archive.

Edinburgh University Archives provides advice and guidance to University staff on identifying records holding archival value and transferring digital records to the University Archive. It ensures records of historical value are preserved for posterity and can be easily accessed.

All staff who create, receive and use University records are required to read and adhere to the Records Management Policy Framework, the Digital Preservation Policy and Collections Management Policy.

The activities and services in this pillar contribute to ensuring the University complies with relevant legislation and accompanying codes of practice on records management.

6.5 Research Support

The University's Edinburgh Research Office works alongside researchers to grow ideas into successful research projects. It owns the University Research Ethics Policy.

The Research Contracts Team advises on all aspects of research contracts, including general data protection matters and compliance with specific funding/grant body requirements regarding the handling of research data and third-party data-sharing agreements.

Each College provides research ethics and integrity guidance tailored to the research it conducts (College of Arts, Humanities and Social Sciences, College of Medicine and Veterinary Medicine and College of Science and Engineering). As part of the ethical review of research projects, School Ethics Review Committees review plans for the collection, use, storage and governance of data.

Ethics Leads are in place in each School to support researchers, including providing advice on the management of their research outputs (i.e. data, information and records). If required, matters relating to information governance can be escalated for further consideration by the University's Research Ethics and Integrity Review Group which ensures the University meets its obligations under the Universities UK Research Integrity Concordat.

The Research Data Service provides researchers with a range of tools and support throughout their research project, including training workshops and online courses on research data management and working with personal and sensitive information. It owns the Research Data Management Policy which must be adhered to by all research staff and postgraduate research students.

The University has very close ties with NHS Lothian. For health research, the joint University of Edinburgh and NHS Lothian Health Board sponsor, ACCORD[1], provides the information governance checks required for sensitive data as part of their sponsorship process.

The Edinburgh International Data Facility provides 'Safe Haven' Services (i.e. Trusted Research Environments) and holds sensitive data, e.g. health research data, in line with external data owner requirements.

6.6 Training and Awareness

The bedrock of the Framework is the understanding and awareness of the University community regarding confidentiality and keeping information safe.

[1] Academic and Clinical Central Office for Research and Development

To that end, all University staff, visitors and postgraduate research students are required to complete online courses in information security and data protection and to retake them every two years.

Students using confidential data sets as part of their study are required to complete the online courses.

Research and research support staff are required to complete an additional 'data protection in research' course.

In addition, the University provides:

- guidance for new students to help them and their data stay protected during their time at the University and a range of information security training materials;
- freedom of information training and guidance for staff on handling freedom of information and subject access requests;
- guidance for staff and guidance for students on the responsible use of AI technology; and
- access to a wide range of other, non-mandatory training courses and learning; resources regarding information management via, for example, its own Digital Skills Programme and free access to LinkedIn Learning.

6.7 Risk Management

Information Risk Management is the ongoing process of identifying, assessing and managing risks to a key University asset, i.e. its information. It is the essence of information governance and as an activity runs through and supports every other element of the Framework.

The Risk Management Framework comprises: the Risk Management Policy and Risk Appetite Statement and the Risk Management Guidance Manual, and is owned by the University's Head of Risk and Resilience.

The University uses a risk management information system to record all University risks, including information risks.

The system enables a risk to be escalated to the highest decision-makers through an online reporting mechanism and to the Risk Management Committee, University Executive and the Audit and Risk Committee. The system can track the actions set to avoid or minimise the risk.

The University has an Internal Audit service which independently assesses the University's risk management arrangements. It reports to and provides assurance to the Audit and Risk Committee that identified risks, including information risks are being managed effectively.

7. Roles and Responsibilities

7.1 All Staff

It is the responsibility of all staff, including honorary staff/associates and contractors, to ensure they are aware of and adhere to the policies that make up this Framework and the other information-related policies listed in Appendix 1.

All staff are responsible for being aware of information risks, bringing areas of perceived risk to a manager's attention, and reporting any incidents that breach University policy or legislation.

In addition, research staff must be aware of and comply with the data protection provisions in the contracts attached to their research projects.

Research staff are also responsible for reporting potential and actual breaches of the data protection provisions of their research contract to their local data protection champion or the Edinburgh Research Office.

The University's standard Terms and Conditions of Employment contractually require staff to be aware of and comply with its policies and practices regarding the use of information technology and the confidentiality and security of information both on and off campus.

7.2 All Students

Students are required to be aware of and adhere to the policies that make up this Framework and the other information-related policies listed in Appendix 1.

They are expected to take all reasonable steps to protect their own data and the University's information when using the University's information-related facilities, services and technology.

In addition, research students must be aware of and comply with the University's Research Data Management Policy and Research Ethics Policy.

They must be aware of and comply with funding/grant body and research contract requirements regarding the handling of research data. They must raise potential and actual breaches of the data protection provisions of their research contract to their academic supervisor.

The University's Code of Student Conduct requires all students to comply with its policies and regulations.

7.3 University Senior Management

Vice-Principal and University Secretary: has overarching responsibility for information governance in the University, is Secretary to the University Court, the University's governing body; has overall responsibility for a range of central professional services, including governance and legal and information compliance.

Vice-Principal and Chief Information Officer: has overall responsibility for the University's IT systems and the value, protection, availability and integrity of University data (excluding research data); leads on the strategy, risk management, investment, policy and oversight of information security, information systems and University data.

Heads of Colleges and Professional Services Groups: accountable for information governance in their College or Professional Service Group; responsibility may be delegated to Heads of Schools/Units and to Heads of Professional Services Departments.

Heads of Schools/Units and Professional Services Departments: responsible, to their Head of College/Professional Services Group, for information governance within their School or Professional Services Department**.**

Principal Investigator/Research Manager/Project Lead: member of staff with responsibility for the intellectual leadership and overall management of a research project, including research data management.

7.4 Specialist/advisory roles

Chief Information Security Officer: leads and owns the University's Information Security Risk Strategy and Information Security Framework.

Head of Information Compliance Services: leads and gives direction to the teams who provide University-wide support with data protection and freedom of information compliance, including information requests and records management.

Information Compliance Manager: leads the central department that coordinates complex freedom of information, environmental information, and subject access requests and provides advice and guidance to University staff on less complex requests and other compliance matters, liaises with the Scottish Information Commissioner's Office.

Data Protection Officer: advises the University on compliance with data protection legislation and monitors its performance against it; owns the Data Protection Policy and Handbook; trains the Data Protection Champions; approves Data Protection Impact Assessments, holds the University Data Processing Register, oversees information breach procedures and liaises with the Information Commissioner's Office.

Records Manager: provides specialist records management advice and expertise to University staff; ensures the Records Management Policy meets legal requirements and is in line with codes of practice and best practice produced by external regulators.

Head of Risk and Resilience: provides risk management advice and assistance, owns the Risk Management Framework, and facilitates the implementation of it across the University; assists with the analysis of operational level risk and the roll-up of significant risks to the strategic level.

University Archivist and Research Collections Manager: leads the multi-disciplinary team of archivists, librarians and curators who manage the University's collections which include archived records; ensures archived records are appropriately stored, preserved and made accessible to users.

7.5 Support roles

Data Protection Champions: staff in Colleges/Schools and Professional Services Groups/Departments who have been trained in data protection; they act as the first point of contact for data protection queries in their area, including giving guidance on data protection impact assessments. When a Data Protection Champion leaves a School/Department, another must be trained to replace them.

Data Stewards: staff in Colleges/Schools and Professional Services Groups/ Departments who are responsible for ensuring the security, access, documentation and quality of the Golden Copy data they are assigned. Their responsibilities include assessing requests for data access and approving the release of data to any third parties.

If external parties are involved, the Data Steward ensures that appropriate data-sharing agreements are in place before data is shared. They maintain records of staff and other systems that have access to their data, and why.

Their role is further described in Information Security Standard 3. Data Stewardship.

Information Security Champions: staff in Colleges/Schools and Professional Services Groups/Departments who help promote good information security practices and act as point of contact for information security in their area. Their role is further described here.

Information Practitioners: staff in Colleges/Schools and Professional Services Groups/Departments who act as the first point of contact for Freedom of Information and Subject Access Requests that relate to their area. When an Information Practitioner leaves a School/Department, another must be trained to replace them. This role is further described here.

8. Review

As part of a cycle of continuous improvement, this Framework was reviewed 12 months from the approval date. Thereafter, it will be reviewed every three years, or sooner if required, for example, to reflect organisational change or material changes to information-related policies. The review will be overseen by the Information Governance Group.

Appendix 1 of Framework
University of Edinburgh Policies Related to Information Governance

All of the policies named below can be found on the University's Policy Directory.

Key Policies
Collections Management Policy (part of integrated Heritage Collections Policy)
Computing Acceptable Use Policy
Data Protection Policy
Digital Preservation Policy
Information Security Policy
Records Management Policy Framework
Research Data Management Policy
Research Ethics Policy
Risk Management Policy and Risk Appetite Statement

Other Information-Related Policies
Account Expiry Policy
Blackboard Collaborate Data Retention Policy
Blogs Retention Policy
Business Continuity Management Policy and Framework
Closed Circuit Television (CCTV) Policy
Forwarding email for ex-staff Policy

Hybrid Workplace Policy
Lecture Recording Policy
Library Collections Policy
Media Hopper Create Notice and Takedown Policy
Media Hopper Create Retention Policy
Social Media, Policy on Employee Use of
Sustainable IT: Personal Computing Devices Policy
Use of Operational Data Policy