Information Governance Framework

1. Introduction

Information is a critical asset for all aspects of University operations and for efficient management of its resources. Information is used as an umbrella term encompassing all university data and content types, including but not limited to structured data; documents and records; research materials and outputs; teaching resources; audio-visual content; and assets such as website content. As well as protecting and providing the right of access to public and personal information, it plays an increasingly strategic role in the way in which Abertay is regulated and held accountable by external bodies such as the Scottish Information Commissioner. Insight and intelligence gathering from our information is key to understanding our institutional position and performance and it therefore plays a key role in the management and governance of the University and its future planning.

Information Governance covers the legal framework such as the Data Protection Act and Freedom of Information and the standards that need to be established to ensure the University's management and security of information operates within the law and the rights of individuals. It concerns all physical and electronic information and its associated systems within the University, as well as information held outside the university that affects its regulatory and legal obligations. Relevant legislation and regulators are summarised in Appendix 1.

2. Purpose

As the steward of this information, the University is responsible for ensuring its management, security, and effective use. The information governance framework facilitates efficient decision making throughout the information lifecycle (Figure 1) and outlines the governance of information as a critical business asset, essential for meeting the University's business, accountability, legal and regulatory requirements. Achieving this requires the cooperation and commitment of all relevant stakeholders (see the section relating to Responsibilities).

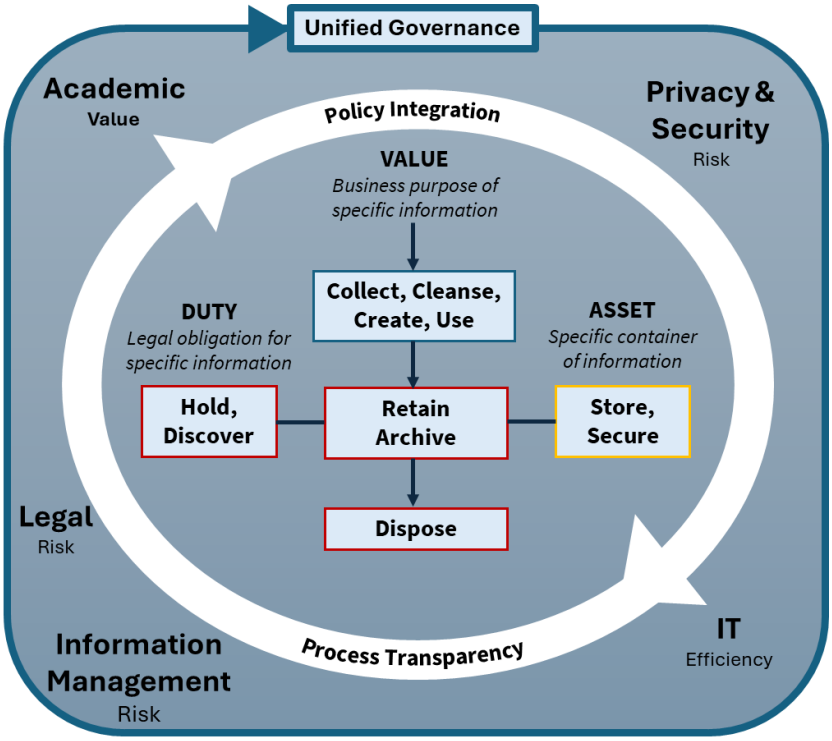

Figure 1 – Information lifecycle

Clear and effective management and accountability structures, robust governance processes, documented policies and procedures, well trained staff and adequate resources are all essential for implementing effective information governance across the University.

3. Scope

The Information Governance Framework documentation is summarised in Figure 2. The University has several policy documents which govern how information is managed and secured during its lifecycle and provide information on what processes are in place to facilitate this.

The University's current information governance policy documents are summarised in Appendix 2. The relevant policy document can be accessed via the University's online Policy Document Library or by emailing policydocumentlibrary@abertay.ac.uk.

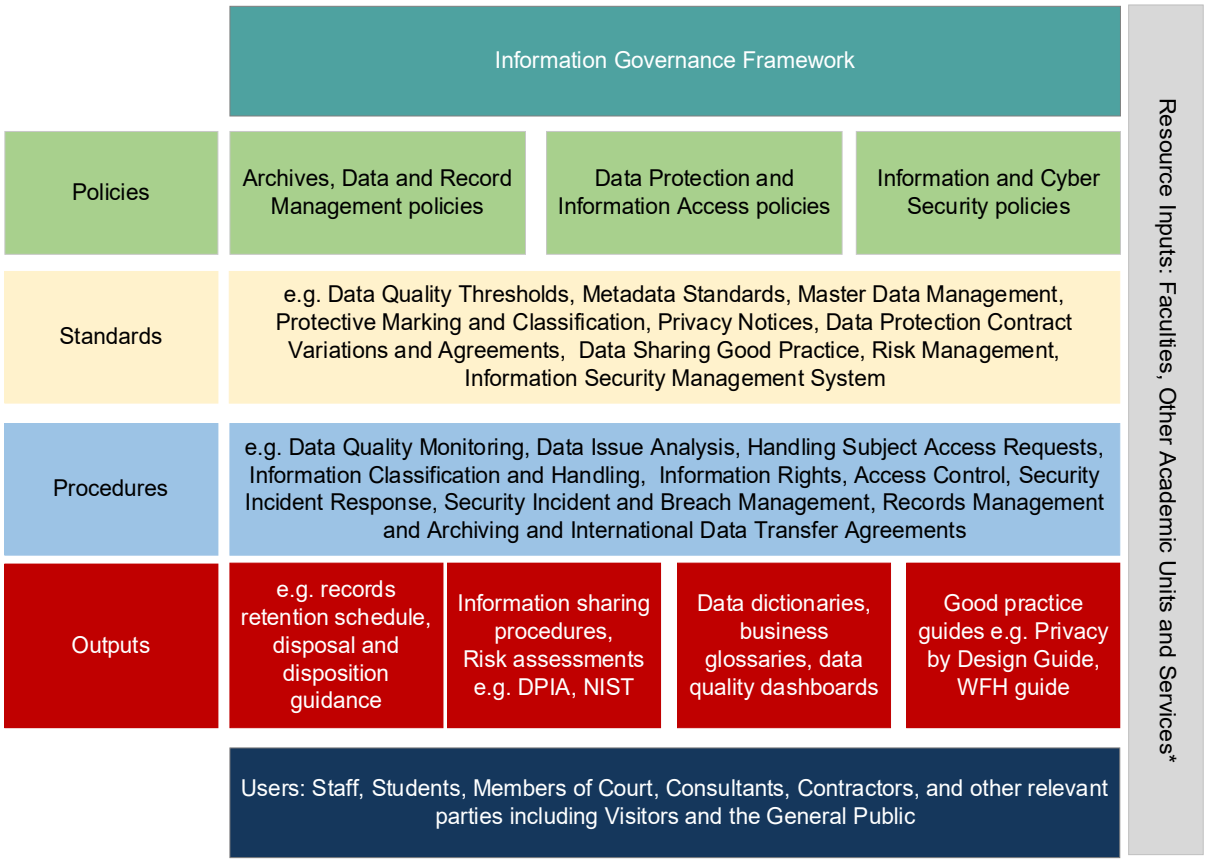

Figure 2: Information Governance Framework Documentation

* Incorporates direct resource inputs from these groups and also indirect resource inputs (e.g. from the general public) via activities conducted by these groups.

Key: DPIA (Data Protection Impact Assessment); DPA (Data Processing Agreement); DSA (Data Sharing Agreement); NIST (National Institute of Standards and Technology); WFH (working from home).

This framework applies to all individuals involved in the information lifecycle, including staff (regardless of contract type), students, members of Court, consultants, contractors, and other relevant parties. It applies to all forms of information whether in hard copy or electronic format processed by or on behalf of the University and covers a wide range of activities, including those involving the use of AI. These activities include, but are not limited to, teaching and education, research, student and staff support, alumni engagement, commercial operations and both internal and external reporting and publications.

4. Principles

Information Governance looks at the whole organisation and users should understand their role in managing information effectively and how effective information management

can only be achieved through collaboration across the University. The framework has information at its heart and reflects the information lifecycle.

The Information Governance Framework aims to:

4.1 General

- Ensure that information governance practices are aligned with university strategic objectives and regulatory requirements.
- Acknowledge the critical role of information in all university activities, by integrating information governance into each stage of the information lifecycle.
- Establish and maintain policy documents for the effective and secure management of its information assets.
- Accurately identify and classify information to ensure that it is handled and shared appropriately.
- Equip individuals with the necessary knowledge and resources to manage information responsibly and effectively. This includes training, functional and secure systems and clear policy documents to support their roles.

4.2 Regulatory Compliance

- Ensure compliance with the Data Protection Act and UK General Data Protection Regulations including maintaining a Record of Processing Activities in accordance with Article 30 of the UK GDPR.
- Ensure privacy notices are in place to provide data subjects with adequate and appropriate information over the way in which Abertay collects, processes, shares information while ensuring the rights of individuals are clearly identified.
- Ensure compliance with the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.
- Ensure adoption of the Model Publication Scheme produced by the Scottish Information Commissioner.
- Ensure statutory reporting (e.g. to Scottish Funding Council and Higher Education Statistics Agency) is accurate and timely.

4.3 Management and Security

- Maintain policy documents for the effective and secure management of its information assets and ensuring ongoing compliance.
- Continually identify all information assets it holds through its Information Asset Registers which will be maintained and reviewed annually.
- Define and enforce access control measures to ensure only authorised users can access sensitive information and minimise risk e.g. embargo breaches such as those imposed on applicant data by UCAS.
- Make data easily accessible to authorised users when needed.
- Establish clear guidelines for classifying and securely handling different type of information.
- Ensure data is accurate, complete, and reliable through regular data quality monitoring, data cleansing and validation processes.
- Ensure data from different sources can be seamlessly combined to provide a unified view.
- Ensure appropriate assessments and audits of its information management and information security arrangements are in place.
- Ensure that key role holders work together to maintain accountability and scrutiny of information governance and security across the University via a formal committee reporting structure.
- Maintain an incident reporting procedure and monitor, investigate and record all reported instances of actual or potential breaches of data privacy, confidentiality and security.
- Ensure that adequate incident response and business continuity plans are in place to give assurance that the University has robust measures to manage and recover from any major disruption to access and use of its information assets.
- Identify and assess information-related risks across the University and developing strategies to mitigate these risks including incident response plans and business continuity plans to minimise impact.

5. Responsibilities

The governance structures, lines of management and risk responsibilities for information governance are outlined below:

University Court

The University Court as the governing body is ultimately responsible for the compliance and security of university information.

Senior Management Team

The Senior Management Team provides a culture of responsible management of information and recognises information as a strategic asset and compliance responsibility. They have overall responsibility for upholding the correct management of information generated by the functions and activities of the various areas of the University.

More specifically, they will ensure that the information and records controlled within their area are managed in a way that meets the aims of the Information Governance Framework and adheres to appropriate information security policies and procedures. By prioritising information governance, the Senior Management Team, helps safeguard the University's information assets against potential threats and vulnerabilities, reduces inefficiencies, and ensures we gain maximal value from our information assets.

Information Asset Owners

Information Asset Owners are responsible for providing leadership and accountability for the management and security of information created, received, and maintained in their areas of the University. They will meet the specifications outlined in the Information Asset Owner and Information Asset Manager Role Specification document.

Data Owners

Data Owners are responsible for the overall management and governance of specific data sets within their domain, including accuracy, security, and proper classification of the data. Data owners also oversee data sharing agreements and coordinate with data stewards to maintain data integrity and security

The role of Information Asset Owner will encompass the role of Data Owner for most data domains.

Information Asset Managers

Information Asset Managers are responsible for dispersing guidance and support to members within their network. Additionally, they are tasked with ensuring that

information security practices are maintained to protect the integrity, confidentiality and availability of information. They will support their Information Asset Owner and the Information Governance Group to deliver the Framework and all related guidance and procedures. They are a crucial link between the Information Governance Group and the wider University, ensuring that information, data, and records management is implemented and monitored universally. An Information Asset Managers Network will enable a culture of sharing and support between and with colleagues.

Data Stewards

Data Stewards are responsible for carrying out the duties delegated by the Data Owner to ensure the accuracy, integrity, and quality of data they work with. They will implement data governance policies and procedures, ensuring compliance with regulatory requirements and university standards including data quality thresholds. Data Steward duties may include data classification, metadata management, and data quality monitoring. They also provide guidance and support to data users, promoting best practices in data handling and usage.

Information Governance Support

Governance, IT Services and the Strategic Planning Office are the main Professional Services that provide support and guidance for all these individuals. Information policies, templates and procedures are managed to ensure they are current and meet statutory requirements.

Data Protection Officer

As a public body, the University is required to appoint a Data Protection Officer in accordance with Articles 37 – 39 of the UK GDPR. Their role is to:

- Inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits.
- Co-operate with and be the first point of contact for supervisory authorities; to engage with individuals whose data is processed by the University.

- Report serious concerns regarding data protection to the highest level of the organisation. Accordingly, they will be able to make such reports directly to Court at any time.

They will receive training as necessary to ensure they remain effective in their role. The Head of Governance and Deputy Secretary is the University's Data Protection Officer and can be contacted by emailing dataprotectionofficer@abertay.ac.uk

Chief Digital Officer

The Chief Digital Officer has a multifaceted and crucial role in maintaining the integrity, confidentiality and availability of the University's information assets.

- Maintaining the information security management system.
- In conjunction with the Data Protection Officer, the development and enforcement of the Information Governance Framework and ensuring that information security measures are integrated into all aspects of information management.
- Overseeing information security risk management activities.
- Ensuring compliance with relevant laws and regulations.
- Promoting information security awareness through training and guidance.
- Monitoring, auditing and reporting of information system compliance.
- Establishing and maintaining security incident response plans.

Users

All users of the University's systems must comply with the University's Information Governance Framework and must handle all personal data and confidential information in a responsible and appropriate way.

In line with statutory timescales as set out in the University's Data Protection Policy, users must report any suspected security incidents and data breaches immediately, following the established reporting procedure to itservices@abertay.ac.uk

Any data protection-related rights requests must be forwarded to the Data Protection Officer by emailing dataprotectionofficer@abertay.ac.uk as soon as possible upon receipt.

All staff should ensure they are aware of their overall role and who to go to for guidance and support, should they need to raise an information and records management issue.

Information Governance Group

The Information Governance Group comprises key roles relating to Information Governance as set out in its terms of reference and has operational responsibility for matters relating to managing information governance, including responsibility for policies, frameworks, risk analysis and strategic initiatives to facilitate best practice across the University.

6. Reporting

The Senior Management Team receives risk assurance from the Information Governance Group around the implementation of effective information risk management including University wide compliance with information management and information security policies and initiatives. The Finance and Corporate Performance Committee receive an annual information governance report.

7. Training and Awareness

The Senior Management Team is responsible for overseeing the provision of effective training for all University staff, and where appropriate, students relating to the management of data, records and information, data protection, security and freedom of information compliance.

The delivery of this framework will require resources and training including mandatory Information Security and Data Protection training for all University members, on an annual basis and targeted training on specific subjects relating to information governance in response to specialist needs. A training needs analysis will be developed working with key stakeholders across the University.

8. Definitions

For the purposes of this framework and related policy documents, terms are defined in the Policy Document Library Glossary.

9. Related Policy Documents and Supporting Documents

Legislation	As listed Appendix 1
Strategy	Digital Strategy
Policy	As listed in Appendix 2
Procedures	As listed in Appendix 2
Guidelines	As listed in Appendix 2
Local Protocol	N/A
Forms	As listed in Appendix 2

10. Additional Information

Audience	Public
Applies to	All University Members
Classification	Corporate Governance
Category	Information Governance
Subcategory	N/A
Approving Authority	University Court
Approval Date	30 April 2025
Effective Date	1 June 2025
Review Date	31 May 2028
Policy Document Author/s	Chief Digital Officer; Head of Governance and Deputy Secretary; Head of Planning and Insight
Policy Document Owner	Vice-Principal and University Secretary

If you would like this document in a different format (e.g. large print, braille), please contact policydocumentlibrary@abertay.ac.uk

If you need any assistance to access or understand the policy, please contact governance@abertay.ac.uk

All printed versions of this document are classified as uncontrolled. Please ensure you access the current version in the Policy Document Library.

Appendix 1 Relevant Legislation and Regulators

The Abertay University Information Governance Framework will ensure compliance with various pieces of legislation relating to the handling and use of information, as well as the common law duty of confidentiality.

Legislation applicable to the Information Governance Framework includes but is not limited to:

Computer Misuse Act (1990). Created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The Act has been modified by the Police and Justice Act 2006.

Copyright, Designs and Patents Act 1988. Grants the creators of original works exclusive rights to control the ways in which their material may be used.

Data Protection Act 2018. The main piece of legislation that governs protection of personal data in the UK and ensure compliance with the European Union GDPR. Requires personal data to be protected through the recognition of data protection principles and extends stronger legal protection for more sensitive personal information.

Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 (DPPEC). This now forms the UK GDPR and amends the DPA 2018 to ensure continued alignment of UK regulations and EU GDPR following the exit of Britain from the EU in 2020.

Environmental Information (Scotland) Regulations 2004. Provides for the accurate reporting of environmental information by Scottish institutions and businesses.

Equalities Act 2010 UK law that protects people from discrimination in the workplace and in society.

Freedom of Information (Scotland) Act (2002). Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner.

General Data Protection Regulations (EU 2018). GDPR and the basis for the UK law below. Compliance with GDPR continues to be relevant to enable EU services and individual's data to be processed appropriately. See DPPEC above.

Human Rights Act (2000) Governs interception or monitoring of communications, most specifically article 8 which guarantees respect for an individuals' private and family life, their home and correspondence. Public authorities cannot interfere with these rights unless it's justifiable to do so.

Intellectual Property Act 2014 Aims to help UK businesses protect their IP rights, and to make the IP system more accessible and efficient

Investigatory Powers Act 2016 UK law that governs how public bodies can use investigatory powers, including: Interception of communications, Equipment interference, Acquisition and retention of communications data, and Acquisition and retention of bulk personal datasets.

National Security and Investment Act 2021 The Act identifies data infrastructure as a sector where transactions could potentially give rise to national security concerns. The definition of data infrastructure includes entities that own, manage, operate, or provide services to data infrastructure, as well as those that support public sector authorities or provide peering, interconnection, or exchange functions for public communications networks and services.

Privacy and Electronic Communication (EC Directive) Regulations (2003). Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover a range of issues relating to privacy in respect of electronic communications including telemarketing and cookies.

Public Records (Scotland) Act 2011 Makes provision about the management of records held by public authorities, including the creation of a records management plan.

Regulation of Investigatory Powers Act (2000). Aims to ensure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.

UK General Data Protection Regulation (UK GDPR) Outlines the rights, obligations, and key principles for processing personal data in the UK, with the exception of intelligence agencies and law enforcement. The UK GDPR incorporates the provisions of the EU GDPR directly into UK law. The core data protection principles, rights, and obligations remain largely unchanged.

Regulators

In addition to legislation, there are a number of codes of practice, issued by Regulatory Authorities, that apply, including:

- Higher Education Statistics Agency
- Information Commissioners Office
- Scottish Funding Council
- Scottish Information Commissioner

Appendix 2 – Information Governance Policy Documents

Abertay University has a number of Policy Documents which govern how information is managed and secured during its lifecycle and provide information on what processes are in place to facilitate this.

The following lists the key Information Governance Policy Documents:

Archives, Data and Records Management:

Policies

- Archives Policy
- Asset management: Control and Disposal Policy
- Data Classification and Handling Policy
- Information and Records Management Policy
- Intellectual Property Policy
- Open Access Publications Policy
- Policy Document Governance Policy
- Research Data Management Policy

Procedures

- Policy Document Governance Procedure

Guidance

- Publication Scheme
- Guidance on Data Protection
- Guidance on Handling Information Requests

Data Protection and Information Access

Policies

- Data Protection Policy
- GDPR for Research Policy
- Individual Rights Policy
- Outsourcing Data Processing and Third Party Access Policy
- Privacy by Design by Default Policy

Guidance

- Research Ethics at Abertay University Guide

Templates and Other Documentation

- Data Processing Agreement
- Data Protection Impact Assessment
- Data Sharing Agreement
- Privacy Notices

Information and Cyber Security

Policies

- Bring Your Own Device Policy
- Email and Messaging Policy
- Information Security Policy
- IT Hardware Asset Policy
- Password Policy
- Physical and Environmental Security Policy
- Software Management Policy
- System Access Control Policy
- Third Party Access to Email or File stores Policy
- Web Filtering Policy

Procedures

- Incident Management Procedures
- Information Security Incident Management Procedures
- IT Operations Security Procedures
- Patch Management Procedure
- Security Incident and Data Breach Reporting Procedure
- Software Application Security Procedure
- Supplier Relationships Procedure
- Systems Vulnerability Management Procedure

- Systems Acquisition, Development and Maintenance Procedure

Guidance

- Information Security Controls Guidance