INFORMATION GOVERNANCE STRATEGY

SUMMARY

Purpose of this document

This Strategy concerns the governance of all information held or processed by the University of Sussex.

Who is this for?

This Strategy and the supporting policies which form the Information Governance Framework are intended for all individuals responsible for the use of information on behalf of the University, and all stakeholders with an interest in how the University manages its information.

The policies that are part of the Information Governance Framework provide specific advice and guidance for those managing and using information on behalf of the University. They include the following key policies which are made available on the University website, and are supported by a suite of policies, procedures and guidance notes:

- Information Classification and Handling Policy;
- The suite of Information Security policies;
- Data protection accountability documents, including the University's Data Protection Policy, Privacy Notice, Record of Processing Activities and the Appropriate Policy Document; and
- Records Management Policy.

Executive Summary

Information governance is the security, control, and optimisation of the information the University uses or holds. The purpose of the information governance strategy is to minimise risks and costs, and maximise the value available from the University's information.

The University recognises that information is a corporate asset. This Strategy formalises the University's commitment to information governance and aims to create an effective, consistent and holistic approach to the governance of information across the University, to support the objectives of Sussex 2025.

All staff, at all levels in the University, have a role to play in the successful implementation of this Strategy. The Strategy sets out those roles and responsibilities, as well as a commitment from the University to ensure all staff have the appropriate training and support to carry out their roles effectively.

Who can you contact if you have any queries about this document?

Any questions about this Strategy should be directed to:

Bridget Edminson, General Counsel and Director of Governance and Compliance
Division of the General Counsel, Governance and Compliance

1. INTRODUCTION

1.1 Information is a foundational asset that enables the student education and experience, research capability and impact, and efficient management of services and resources. It is therefore important to ensure that information is effectively managed, and that appropriate policies, procedures and management accountability are in place to provide a robust Information Governance Framework.

1.2 Information governance allows organisations and individuals to ensure that information is handled legally, securely, efficiently and effectively, in order to deliver the best outcomes. It is concerned with how information is held, obtained, recorded, used and shared by an organisation.

2. SCOPE

2.1 This Strategy is concerned with the University's information governance in its broadest sense: its documentation and activities, and its policies, particularly those relating to information handling, information security, data protection and records management. The University's Information Governance Framework is defined in greater detail later in this document. It applies to all University staff, contractors and consultants, regardless of employment terms, position and location.

2.2 The Information Governance Framework applies to all the University's information assets, including:

- the collection of data concerned with our students, staff, research, customers, suppliers, visitors, enquirers, applicants, collaborators and funders;
- information created to support business activities; and
- applications, programmes and systems used to create, capture and maintain information.

2.3 Throughout this document, all the University's records, information and data holdings are described holistically by the term 'information'. The majority of information in future will be created, managed and preserved digitally. However much historic information is still paper-based. This Strategy applies to all information regardless of medium, although priority should be given to developing digital solutions and enablers. It is also intended that the document prepares for, and complements, a future University Data Strategy.

3. AIMS

3.1 The aims of this Information Governance Strategy are to:

- ensure that information governance supports the delivery of the University's Sussex 2025 strategy;
- ensure compliance with all relevant information governance legislation and codes of practice;
- keep our confidential business information secure, protected from unauthorised access, and only disclose it in the course of official business;
- ensure that information utilised by the organisation is available to the right people at the right time;

- ensure that 'the right way' is the easy way, and that staff are aware of their responsibilities;
- instil an information governance culture within the University so that it is part of everyday business;
- ensure that privacy and security by design is incorporated into new projects;
- minimise financial and reputational risks relating to data losses or inappropriate processing of information;
- provide stakeholders with appropriate assurance with respect to the current level of compliance with information governance requirements and best practice.

4. INFORMATION GOVERNANCE STRATEGY GUIDING PRINCIPLES

4.1 This Information Governance Strategy was developed following consideration of best practice in UK higher education, other sectors, and use of international benchmarking. The UK higher education policy and regulatory context was also considered. The Strategy aims to enable the University to respond to existing requirements and upcoming regulatory changes such as those that may be generated by the UK Government Taskforce on Innovation, Growth and Regulatory Reform.

4.2 Studies of best practice identify the characteristics of effective University information governance. The Information Governance Strategy proposes actions for further development in terms of these capabilities. These are:

1. **It is an institution-wide issue -** The sheer scale of information processed and used by universities, combined with a more active and extensive regulatory environment mean that the risk is a corporate-level one and not one that can be managed by any individual department.
2. **Leaders are accountable -** good practice guides to information governance identify senior team leadership as the most important factor in effective information governance.
3. **It is viewed as an institutional requirement (cost of doing business) -** information governance is a foundational activity that enables the delivery of the University's objectives. Business as usual activities, active projects and programmes that have a significant information management component are all 'in scope' for the University's information governance.
4. **It is aligned to university strategy -** and supports the delivery of Sussex 2025.
5. **Information governance is not a project** - but a permanent component of effective university management which should operate with a 'continuous improvement' approach.
6. **It is risk-based -** integrated with the University's risk management processes, with the evaluation of risks and mitigations helping to determine information governance priorities.
7. **Roles, responsibilities, and segregation of duties are defined -** information touches on all areas of the University. Our business processes generate greater volumes of information than ever before. A 'team' approach is needed to deliver good information governance, with every participant aware of their role, the role of others, with the University providing mechanisms and support to enable them to collaborate effectively.
8. **It is addressed and enforced in policy -** a comprehensive suite of policies is required that address the detailed requirements of regulators and UK law. They must assure the

University's Council (through Audit & Risk Committee) that the institutional reputation is protected and provide a level of assurance to key stakeholders and partners, including the student community and wider society.

9. **Adequate resources are committed -** the scale and extent of the information managed by a contemporary university, and the complexity of the regulatory framework requires a higher level of resourcing than the historical norm.
10. **Staff are aware and trained -** rates of engagement with training have improved at the University in recent years, to reach a high level of compliance. It is good practice to regularly review quality of training and engagement.
11. **A development life cycle is required -** security risks and events occur throughout a system's lifetime, be that paper-based records or those held within an IT system, whether the system is developed internally or purchased for on premise hosting or is a cloud implementation. Security should be embedded throughout all phases of the IT system development life cycle, assessed during system acquisition processes, and monitored during system maintenance, including disposal.
12. **It is planned, managed, measurable and measured -** a planned and managed system that has performance measures can provide reliable assurance regarding information governance effectiveness, levels of regulatory compliance, and ability of staff and departments to address security issues for which they are responsible. Metrics can also help identify levels of risk in not taking certain mitigation actions and, in that way, provide guidance for prioritising future resource investments.
13. **It is reviewed and audited -** regular review and audit of information governance policies is a standard part of UK higher education governance, to encourage review of and benchmarking of practice, to provide assurance that there is compliance with the legal and regulatory codes that the University is subject to, and that its reputation is being well managed.

5. INFORMATION GOVERNANCE STRATEGY OBJECTIVES

5.1 The level of maturity of information governance in the University in July 2021 is between level 3 (Defined) and Level 4 (Quantitatively Managed) on a five-point scale[1]. There is, as would be expected, variation of levels across the individual maturity assessment criteria.

5.2 Building on the University's existing information governance capability, **the objectives of this strategy are** that:

1. the University further develops its Information Governance Framework, and takes a holistic approach to information governance, with consistent roles and responsibilities being identified and cited by the component policies that constitute the University's approach to information governance;
2. understanding and oversight of the Information Governance roles and responsibilities (including Senior Information Risk Owner (SIRO), Data Protection Officer, and the role of all staff members) is further developed and is used to inform training and development;
3. a 'continuous improvement' approach measures performance and benchmarks against best practice elsewhere in the higher education sector;
4. the University's information governance will adapt to a changing environment through monitoring and awareness of upcoming legislative and regulatory requirements;

[1] This is based on a comparison against the European Archival Records and Knowledge Preservation project Maturity Model for Information Governance.

5. cyber-security and accessibility will be primary considerations in design of University business processes and systems; and
6. systems will be simplified and standardised where possible, enabling connections that encourage people to collaborate more closely and with more consistency.

5.3 The Strategy will deliver **benefits** from increased efficiencies and reduced risk through:

- improved control of valuable information assets;
- proactive compliance with legislation and standards;
- building confidence with stakeholders as a trusted business partner;
- better use of staff time though ease of location and retrieval;
- better use of physical and server space; and
- reduced costs of business processes and better services through more effective use of information ('make once use many').

6. INFORMATION GOVERNANCE FRAMEWORK

6.1 The Information Governance Framework comprises people, principles, policies and technical and organisational controls to help protect information, promoting openness but mindful of the needs and rights of individuals who entrust their personal data to the University and the requirements of other interested parties including funding and regulatory bodies.

6.2 Taken collectively, the existing suite of policies form a nascent Information Governance Framework. The parent-child arrangement of policies and associated procedures and guidance is helpful for navigation, and the policies are easily located on the University webpages. There is scope to further develop the University's information governance maturity through drawing together the existing suite of policies into a general framework that is informed by this Information Governance Strategy.

6.3 External drivers of the Information Governance Framework include the requirements of the Committee of University Chairs Higher Education Code of Governance that '*high-quality and robust data is produced and managed to meet all relevant legal and regulatory requirements*', and notes that the governing body must assure itself that it has '*effective arrangements in place for the management of information which meet ethical standards, Freedom of Information requirements and other legislation on the use and protection of data*'. Institutions are instructed to '*publish accurate and transparent information which is widely accessible*'.

6.4 Similarly, the Office for Students identifies Public Interest Governance Principles that apply to all registered providers, which include:

- Accountability: The provider operates openly, honestly, accountably and with integrity and demonstrates the values appropriate to be recognised as an English higher education provider; and
- Risk management: The provider operates comprehensive corporate risk management and control arrangements (..) to ensure the sustainability of the provider's operations.

6.5 The Information Governance Framework provides the basis for the creation, capture, management and use of full and accurate records, information and data in all formats used by the University. It describes how information is to be governed as a vital business asset which is essential to help meet the University's business, accountability, legal and regulatory requirements.

6.6 The Information Governance Framework includes the following key policies which are made available on the University website, and are supported by a suite of policies, procedures and guidance notes:

- Information Classification and Handling Policy;
- The suite of Information Security policies;
- Data protection accountability documents, including the University's Data Protection Policy, Privacy Notice, Record of Processing Activities and the Appropriate Policy Document; and
- Records Management Policy.

6.7 The Information Governance Framework outlines an approach to information governance integrated with other organisational governance such as audit, accountability, compliance, risk management, business continuity, security and IT governance. The requirements of this framework are informed by the University's business environment, legislation, strategy and supporting policies.

6.8 The Information Governance Framework also describes the cooperation and commitment required from all relevant stakeholders for implementation of effective information governance across the University. This will support the delivery of Sussex 2025, and mitigate institutional risks such as those relating to cyber security, data breaches, and non-compliance with legislation.

Information Culture

6.9 The University's information culture is a key part of the Information Governance Framework. The information culture describes the way in which Information Governance is perceived, valued and embedded across all levels of an organisation. An empowered and effective implementation of this Strategy should result in a positive and proactive information culture, indicators of which include:

- effective induction, training & awareness raising;
- staff value the information with which they work;
- staff understand the importance of managing information correctly and consistently;
- poor practice is challenged;
- managers lead by example;
- staff feel confident to ask questions and safe to raise concerns; and
- information governance is considered when designing new systems and processes, or as a key part of any new project.

Roles and Responsibilities

6.10 Specific roles and responsibilities relating to individual University policies are described within the relevant policy documents. In terms of the Information Governance Framework, the University's expectations is that all staff are responsible for complying with the requirements of the framework. The following also have specific responsibilities:

Council

6.11 The University's governing body is responsible for oversight of the University's information governance. Scrutiny of the University's information governance outcomes is usually delegated to Audit & Risk Committee. Audit & Risk Committee will receive an annual update of the University's information governance key performance indicators, including a summary of information governance training compliance. The Committee will also receive all formal information governance audit reports.

University Executive Group

6.12 The University's Executive Group (UEG) will receive reports and recommendations for action from the Senior Information Risk Owner (SIRO). Direct reporting to UEG and Audit and Risk Committee is in line with requirements laid out in the Information Commissioner's Office's Accountability Framework, which requires that there should be clear reporting lines and information flows, with the highest senior management level having overall responsibility for data protection and information governance.

6.13 Where approved, UEG will oversee implementation of actions and measures required to ensure continued compliance with Information Governance policy and legislation.

Senior Information Risk Owner

6.14 The Senior Information Risk Owner (SIRO) is a University Leadership Team member who provides focus for the management of information risk across the University. The SIRO's role is to lead and foster a culture that values, protects and uses information for the success of the University and benefit of its stakeholders. The SIRO is responsible for the University's information risk and incident management framework, ensuring information risks and incidents are appropriately managed.

Data Protection Officer

6.15 The Data Protection Officer (DPO) is responsible for monitoring internal compliance with data protection legislation, informing and advising on data protection obligations, providing advice in relation to Data Protection Impact Assessments, and acting as a contact point for data subjects and the Information Commissioner's Office (ICO) (including reporting personal data breaches on behalf of the University).

7. DELIVERY OF THIS STRATEGY

7.1 This Strategy will be delivered through an annual Information Governance Work Plan outlining how the University will meet requirements under the Strategy, taking account of national information governance policy, guidance, standards and legislation.

7.2 Effective monitoring plays a key role in the successful delivery of the Strategy and the University's Information Governance Framework will be subject to scrutiny at appropriate levels by both internal and external stakeholders.

7.3 The University's Executive Group will evaluate the effectiveness of the Information Governance Strategy through the review of key indicators of performance. It will also receive an update of the Information Governance Work Plan on an annual basis.

Key Performance Indicators

7.4 Key performance indicators demonstrate to stakeholders and regulators that the investment in and focus on Information Governance is making a difference and improving the University's information governance capability and reducing risk. They also help inform conversations about future priorities.

7.5 They are a mix of input and output information governance indicators.

7.6 The following Information Governance Key Performance Indicators will be reported to the University's Executive Group annually:

- Completion of any mandatory Information Governance training to include data protection training and information security training;
- Information Security incidents by type;
- Completion of (risk based) records management audits and outcomes;
- Data subject requests – number and average turnaround time; and
- Freedom of Information Requests - number and average turnaround time.

7.7 A time series will be provided to highlight the direction of travel, along with a commentary to provide further context. In some cases, good practice in information governance could produce counterintuitive outcomes in terms of the metrics, such as improved reporting rates of information security incidents could mask a level or declining trend in the actual number of incidents. The subject matter expertise of the SIRO, DPO and the Director of IT Services will inform the explanatory information that accompanies the key performance indicators.

7.8 An annual Information Governance Strategy report will be provided to Audit and Risk Committee.

8. INFORMATION GOVERNANCE STRATEGY MILESTONES

8.1 The following Information Governance Strategy milestones are identified for each academic year. Progress against these will need to be reviewed by the UEG. In subsequent years the UEG will need to review these milestones to ensure that they are still appropriate to enable the University to achieve the desired level of information governance.

21/22:

- Develop and begin implementation of a communications plan for information governance, with focus on the Information Governance Strategy and Framework.
- Induction for new staff to include detail about the Information Governance Strategy and Framework.
- Develop one home web page for the Information Governance Framework, with signposting to supporting documentation.
- Implement mandatory information security training for all staff.
- Roll out of mandatory refresher data protection training for all staff and continued compliance with data protection training requirements for all new staff.
- Termly report to UEG in relation to Information Governance training compliance.
- Annual refresh of policies within the Information Governance Framework.

- SIRO will review the University's information governance risks and feed them into the University's corporate risk management processes.
- Support any audit of Information Governance related policies and procedures.
- Annual Information Governance Strategy report provided to UEG and Audit and Risk Committee.
- Support the development of a Data Strategy, begin implementation.

22/23 and ongoing:

- Continued implementation of the Information Governance communications plan.
- Further develop the maturity of the Information Governance Framework through review and harmonisation of policies.
- Continued completion of required Information Governance training and termly report to UEG in relation to training compliance.
- Develop a single RACI Model of roles and responsibilities across the whole Information Governance Framework.
- SIRO will review the University's information governance risks and feed them into the University's corporate risk management processes.
- Support any audit of Information Governance related policies and procedures.
- Annual Information Governance Strategy report provided to UEG and Audit and Risk Committee.
- Complete the implementation of the Data Strategy.

Review / Contacts / References	
Title:	Information Governance Strategy
Date approved:	15 November 2021
Approving body:	University Executive Group
Last review date:	15 November 2021
Revision history:	N/A
Next review date:	15 November 2022
Related internal policies, procedures, guidance: • Sussex 2025 Strategy • Ahead of the Digital Curve, The Sussex Strategy – Digital and IT • Information Classification and Handling Policy https://www.sussex.ac.uk/webteam/gateway/file.php?name=information-classification-and-handling-policy---feb-21-final.pdf&site=76 • Data Protection accountability documents and webpages http://www.sussex.ac.uk/ogs/policies/information/dpa • Information Asset Owners & Information Asset Register http://www.sussex.ac.uk/ogs/policies/information/dpa/iaos • Information Security Policies https://www.sussex.ac.uk/infosec/policies • Records Management Guidance http://www.sussex.ac.uk/ogs/policies/information/recordsmanagementguidance	
Strategy owner:	Professor David Maguire, Interim Vice-Chancellor
Lead contacts:	Bridget Edminson, General Counsel and Director of Governance and Compliance (Senior Information Risk Owner).

	Jason Oliver, Director of IT Services. Alexandra Elliott, Head of Information Management and Compliance (Data Protection Officer).