INFORMATION GOVERNANCE FRAMEWORK

1. Introduction

1.1. This Information Governance Framework (the 'IG Framework') and its associated policies aims to set out the principles and responsibilities relating to the creation, capture, management and use of records, information and data in all formats used by and on behalf of 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.

1.2. Information Governance comprises Information Management and Information Security and must be integrated with other organisational governance such as audit, accountability, compliance, risk management and business continuity. Clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources are all essential to implement effective Information Governance across the University.

1.3. Information is a key asset for the University and as such the IG Framework requires cooperation and commitment from all relevant stakeholders.

2. Scope and definitions

2.1. The IG Framework applies to all employees, regardless of contract type; consultants; contractors; research students and other relevant parties processing information on the University's behalf.

2.2. The IG Framework applies to all information processed by or on behalf of the University, (whether hard copy or electronic) including, but not limited to, the provision of teaching and education, research, student and staff support, commercial activity, internal and external reporting and publications.

2.3. A glossary of the terms used throughout the Framework can be found here

3. Principles

The University will adopt the following principles in the design and implementation of the IG Framework:

3.1. General

3.1.1. The University will establish and maintain policies and procedures for the effective and secure management of its information assets

3.1.2. The University will accurately identify and classify information to ensure that it is handled and shared appropriately, in line with the University Data Classification and Handling Policy.

3.1.3. Those with an operational need will be given the necessary knowledge and resources to manage information responsibly and effectively, including training, functional and secure information systems and clear policies and guidelines.

3.1.4. Information is integral to all business and academic activity and therefore the University will ensure that Information Governance will be considered at all stages of processing.

3.2. Regulatory Compliance

3.2.1. The University will implement policies to assist compliance with the Freedom Of Information Act and the Environmental Information Regulations.

3.2.2. The University will implement policies to assist compliance with the Data Protection Act and UK General Data Protection Regulations.

3.2.3. The University will maintain Records of Processing Activities in accordance with Article 30 of the UK GDPR.

3.2.4. Mandatory Information Security training must be undertaken by all staff on an annual basis.

3.2.5. The University will ensure appropriate privacy notices are in place to provide data subjects with adequate and appropriate information over the way in which the University collects, processes, shares information while ensuring the rights of individuals are clearly identified.

3.3. Management and Security

3.3.1. The University will maintain policies, procedures and standard operating procedures (SOPs) for the effective and secure management of its information assets; ongoing compliance with these will be overseen in line with paragraph 3.3.4.

3.3.2. The University will continuously identify all the information assets it holds through its Information Asset Registers, which will be maintained and reviewed annually.

3.3.3. The University will arrange appropriate assessments and audits of its Information Management and Information Security (including cyber security) arrangements.

3.3.4. Key roles, as defined in paragraph 4, will work together to ensure appropriate accountability and scrutiny of Information Governance across the University via a formal committee reporting structure.

3.3.5. The University will maintain incident reporting procedures and monitor, investigate and record all reported instances of actual or potential breaches of data privacy, confidentiality and security.

3.3.6. The University will ensure that adequate business continuity plans are in place to give assurance that it has robust measures to cope with potential major disruption to access and use of its information assets.

4. Roles, Responsibilities and Reporting

Annex A sets out key roles with responsibility for the implementation of effective Information Governance across the University. The roles and related responsibilities are set out below:

4.1. Senior Information Risk Owner (SIRO)

The SIRO Role is to:

4.1.1. take the lead on delivering risk management and security strategy and assist senior management in the delivery of this including chairing the Information Governance Group (IGG).

4.1.2. oversee security, incident and risk management and reporting.

4.1.3. escalate and advise on any significant issues affecting Information Governance, risk and security to senior management.

4.1.4. The SIRO shall receive training as necessary to ensure they remain effective in their role.

4.2. Data Protection Officer (DPO)

As a public body, the University is required to appoint a DPO in accordance with Articles 37 – 39 of the UK GDPR. The DPO Role is to:

4.2.1. Inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws.

4.2.2. 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.

4.2.3. To co-operate with and be the first point of contact for supervisory authorities; to engage with individuals whose data is processed by the University.

4.2.4. The DPO shall receive training as necessary to ensure they remain effective in their role.

4.2.5. The DPO must be able to report serious concerns regarding data protection to the highest level of the organisation. Accordingly, the DPO will be free to make such reports directly to Council at any time.

4.3. Caldicott Principles

The University will abide by the eight Caldicott Principles where it processes patient data as part of its Research output. The Head of Project Assurance (Research) will have oversight of the integration of these Principles and, alongside the Research Integrity Manager, will work alongside the Data Protection Officer and wider Information Governance Group to offer assurances.

4.4. Information Asset Owner (IAO)

4.4.1. The most senior member of staff of a Directorate or Faculty, IAO's are accountable to the SIRO for the Information Assets within their area and for ensuring effective management of any risks associated with the handling of information assets as detailed in their Information Asset Register.

4.4.2. IAO's must ensure information assets are handled and managed appropriately. This includes ensuring information assets are properly protected against risk and that their value to the organisation is recognised.

4.4.3. IAOs shall receive training as necessary to assist them in their role.

4.5. Information Asset Manager (IAM)

4.5.1. Designated by, and responsible to, the relevant IAO, Information Asset Managers are individuals with operational responsibility for specific information assets. They are business users with expert knowledge of business processes and how data is used within those processes.

4.5.2. The IAM's role is to be responsible for the maintenance of Information Asset Registers in their area, to raise any information management issues and risks to the IAO, monitor completion of mandatory Information Security training and to ensure staff are aware of best practice and compliance requirements.

4.5.3. The IAMs may nominate individuals to provide administrative support to the IAMs as necessary.

4.5.4. The IAMs and their nominees shall receive training as necessary to assist them in their role.

4.6. Information Governance Champions (IGC)

4.7.1 IGCs are individuals appointed by IAOs and/or IAMs to act as a first point of contact regarding Information Governance issues in their respective areas.

4.7.2 The IGCs role involves undergoing specific training in Information Governance in order to equip role holders to provide advice to colleagues locally, signpost to relevant polices and procedures and to aid in recognising potential issues that may need to be escalated.

4.7.3 IGC's should identify and report Information Governance issues and risks to their respective IAM and disseminate Information Governance training, messages, guidance and best practice within their area.

4.7. Users

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

4.7.2. 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 and forward any data protection-related rights requests to the Legal and Information Compliance team as soon as possible upon receipt.

4.7.3. Where required, users will undertake mandated annual Information Security training.

4.8. Information Governance Group (IGG)

4.8.1. The IGG 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. The Information Governance Group is overseen by the Risk and Compliance Group.

4.9. Reporting

4.9.1. The Risk and Compliance Group (RCG) receives risk assurance from the Information Governance Group and oversees and monitors on behalf of the University Executive Committee (UEC) the implementation of effective information risk management including University-wide compliance with Information Management and Information Security policies and initiatives.

4.9.2. Audit and Risk Committee (ARC) will receive annual reports from the Information Governance Group detailing the University's Information Governance risk management activities, which informs the Committee's annual report to Council.

5. Associated Policies and Procedures

5.1. This Framework sets out the high-level principles and policies for Information Governance across the University. Associated policies pertaining to Information Governance sit under this policy; these are not exhaustive and are set out in Annex B.

6. External Legislation

6.1. The University's IG 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 IG Framework includes but is not limited to:

6.1.1. UK General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA18)

6.1.2. Human Rights Act 1998 (HRA98)

6.1.3. Freedom of Information Act 2000 (FOI) / Environmental Information Regulations 2004 (EIR)

6.1.4. Computer Misuse Act 1990

6.1.5. Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)

6.1.6. Copyright, Designs and Patents Act 1988

6.1.7. Malicious Communications Act 1988

6.1.8. Intellectual Property Act 2014

6.1.9. Investigatory Powers Act 2016

6.1.10. Regulation of Investigatory Powers Act 2000

7. Review, Approval & Publication

7.1. The IG Framework will be reviewed, at a minimum, every two years. The IGG is responsible for such review;

7.2. The IG Framework will require approval by the University Executive Committee (UEC) and will then be published on the University website within the Policy Zone.

8. Annexes

8.1. Annex A sets out the Information Governance roles interactions.

8.2. Annex B sets out the overall structure of the Information Governance Framework documentation.

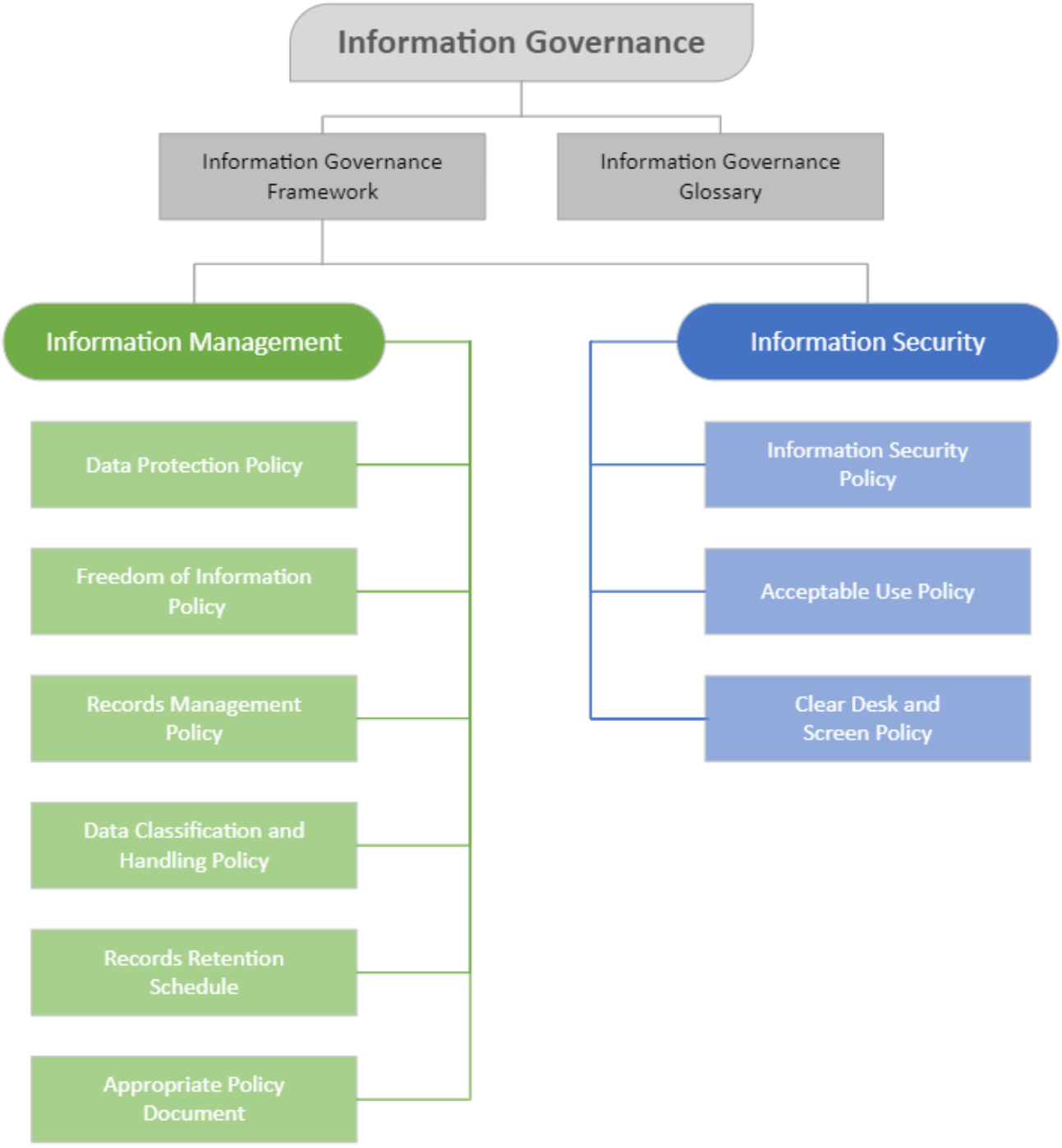
9. Document Control Information

Document Name	Information Governance Framework
Owners	Director of Legal, Governance & Compliance (LGC), Associate Director, Projects & Service Assurance (IDS)
Version Number	2.0
Equality Analysis Decision and Date	Not applicable
Approval Date	30th May 2022
Approved By	UEC
Date of Commencement	19th September 2019
Date of Last Review	30th May 2022
Date for Next Review	30th May 2024
Related University Policy Documents	Data Protection Policy Information Security Policy Records Management Policy Freedom of Information Policy Data Classification and Handling Policy Appropriate Policy Records Retention Schedule Acceptable Use Policy Clear Desk and Screen Policy
For Office Use – Keywords for search function	Information governance, data protection, privacy, information security, cyber security, information management, governance, UK GDPR, General Data Protection Regulation, PECR, Data Protection Act 2018, IGG, SIRO, DPO, Caldicott Guardian, DPIA, IG Champion, IAO, IAM, risk and compliance, RCG, framework, regulatory compliance

ANNEX A

Information Governance Role Interactions

ANNEX B


Information Governance
Information Governance Framework
Information Governance Glossary
Information Management
Information Security
Data Protection Policy
Freedom of Information Policy
Records Management Policy
Data Classification and Handling Policy
Records Retention Schedule
Appropriate Policy Document
Information Security Policy
Acceptable Use Policy
Clear Desk and Screen Policy