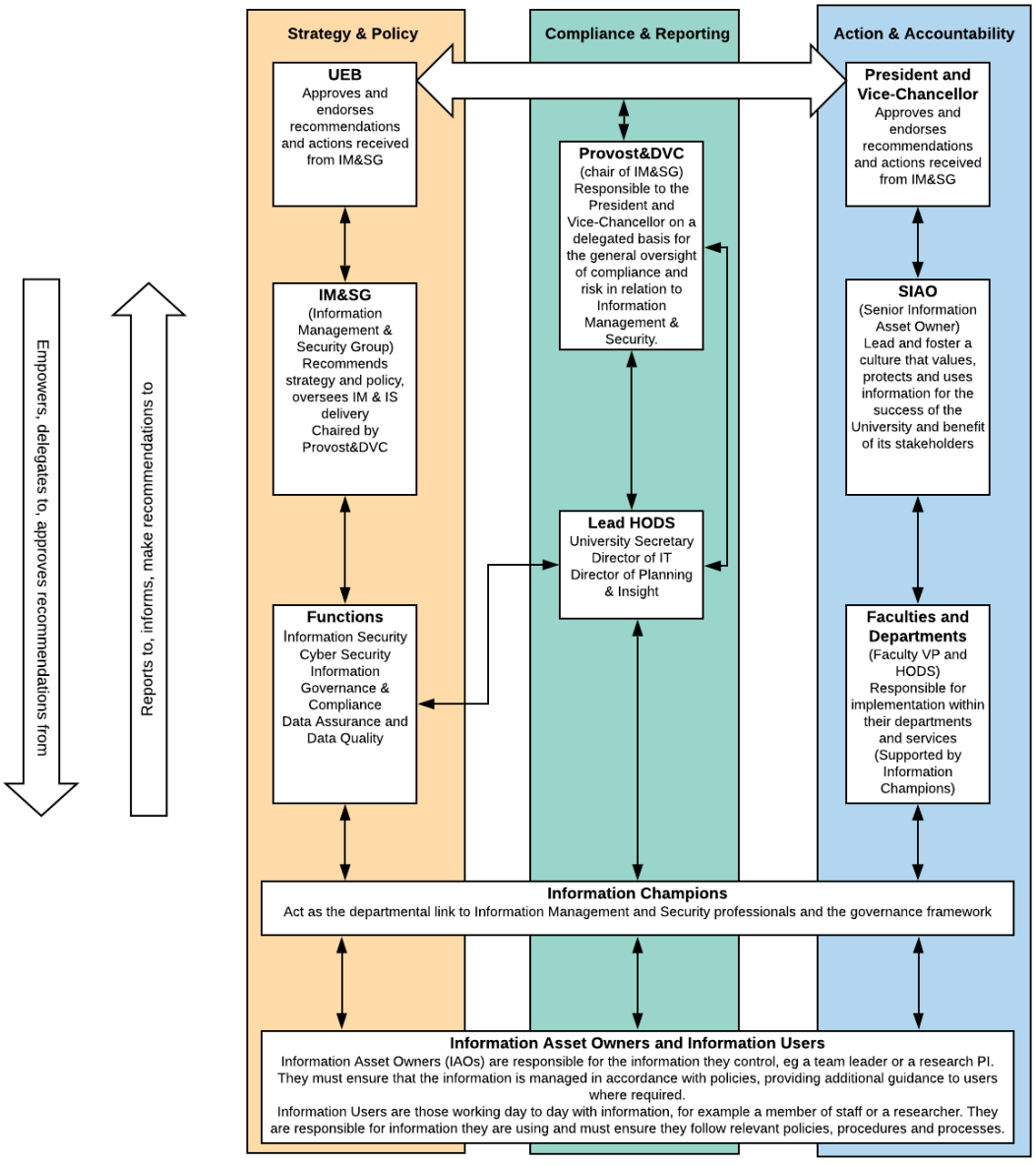
Roles and Responsibilities for Information Governance (Updated March 2020)

Figure 1. Structure for Information Management and Security Governance. It is intended the structure will provide an immediate core framework for information management governance within the University with recognition that this can be refined and can evolve in response to future internal and external requirement.



Roles and responsibilities

Strategy and Policy

University Executive Group (UEB)
University Executive Board considers the necessary strategies and policies on the recommendation of Information Management Group (IMG), or to be agreed by IMG where it has the delegated authority. The University Secretary will report to UEB on the degree to which the University is compliant, the actions required and the residual risks that exist where further action is needed and make recommendations.

UEB Information Management and Security Group (IM&SG)
Accountability for recommending policy, monitoring and reporting on compliance and reporting risk has been delegated through UEB to the IM&SG. IM&SG, comprises of the following. Provost and Deputy Vice Chancellor (chair); UEB SIRO; CISO; University Secretary; Executive Director of Academic Services; Executive Director of Professional Services; Director of IT; Director of Planning and Insight; two senior academics with subject matter expertise recommends policy to UEB and oversees delivery with support from the Information Management Operations Group and Data Governance Group. IM&SG will provide the strategic direction and oversight required to ensure a consistent framework of policies and procedures encompassing the storage, retention, structure, use, protection and gaining value from information assets in relation to the strategy and purposes of the organisation while meeting our regulatory and statutory requirements.

Technology: Cyber-security is the responsibility of the Director of IT and focuses on the technical measures to protect computer systems from unauthorised access or being otherwise damaged, corrupted or made inaccessible (whether or not they hold personal data.)

Information Security: is the responsibility of the UEB nominated Senior Information Risk Owner (SIRO) and is a broader category that looks to introduce measures to protect all information, whether in hard copy or in digital form from unauthorized/inappropriate access, use or disclosure, including high value assets, e.g. intellectual property and research data. Its scope covers people, process and technology and is designed to provide whole-university protection of assets with value.

Regulatory Compliance: is the responsibility of the University Secretary and includes the General Data Protection Regulation (GDPR), which addresses the rights of individuals in relation to information held about them and the legal duties placed on the University. It includes but is not limited to the security of personal data.

Data Quality, Data Structures and Reporting: is the responsibility of the Director of Planning and Insight. This includes external and internal reporting on corporate information for regulatory, administrative and planning purposes, data definition, data dictionary management, definition and control of how data is structured within systems, management of reference data including consistent coding structures across systems, data quality assurance and responding to the reporting requirements of the designated data body and other statutory customers as well as meeting internal user-defined requirements for reporting.

UEB IT sub-group
The IT sub-group to UEB has strategic oversight of the programme of IT system projects at University level; keeping business cases under review, recommending projects to UEB, monitoring project progress, risks and benefit realisation. The University Secretary is a member of the UEB IT Group and the Director of Information Technology is a member of IMG. Where IT projects require information governance policies or need to comply with information governance requirements (e.g.

Data Protection Impact Assessments) reference will be made to IMG. Where IMG require a system solution to achieve greater compliance (e.g. Cyber Security) reference will be made to UEB IT Group.

Compliance and Reporting

Provost and Deputy Vice Chancellor
Chair of the IM&SG. Responsible to the President and Vice-Chancellor on a delegated basis for the general oversight of compliance and risk in relation to Information Management and Security.

University Secretary
The University Secretary is responsible to the President and Vice-Chancellor on a delegated basis for the oversight of compliance with legal and regulatory requirements and the associated risks in relation to information governance. As the University Secretary is independent and not an information asset owner they are not subject to a conflict of interest. The statutory functions of the Data Protection Officer sit with or are accountable to the University Secretary.
Faculties and Departments remain responsible for compliance with data protection law and must be able to demonstrate compliance.

Data Protection Officer (DPO)
The DPO will act in an advisory role, liaising with Faculty and departments to help them ensure compliance with data protection provisions. The DPO will provide information and guidance on the processing of all personal data. They will produce guidance material for staff and deliver training to staff. Process, co-ordinate and respond to all requests for information and deal correctly with subject access requests. Be the point of contact for data subjects and for cooperating and consulting with national supervisory authorities.

Action and Accountability

President and Vice-Chancellor
Responsibility for action and implementation ultimately rests with the Council, through the President and Vice-Chancellor.

Accountable Officers
The Executive Director of Academic Services, Executive Director or Corporate Services and the Chief Financial Officer are accountable officers for the management and use of information systems, data management and processing at the University and for fostering a culture for using and protecting data, that information is accurate and its value is realised, information is secured and legislation is complied with. The Executive Director for Corporate Services owns the University's information incident management framework.

Senior Information Asset Owners
Those who have responsibility for a process or system (typically Directors of Professional Services) are the Senior Information Asset Owners and are responsible for knowing what information the asset for which they are responsible holds, what information is transferred in and out of it and what systems it links to, who has access and why and ensures their use is monitored and compliant with the appropriate policies. The SIAO is responsible for reporting any incidents of a breach of policy, data security or data protection. The Senior Information Asset Owner will be the **Data Steward** for the data held in the asset for which they are responsible. A Data Steward is accountable for managing systems and processes. They must have the authority and means to manage the data for which they are accountable and these responsibilities should be set out in their job description. They have responsibilities to:

- Review and document data management practices for key datasets.
- Define data governance roles and include in role descriptions.
- Ensure that policies for systems and the data they hold are clear and aligned across the University.
- Develop reporting which enables data value to be realised through regular reporting of insight to the wider University.
- Undertake reconciliation of datasets to merge data from standalone systems and decommission where possible.

Faculties and Departments

Faculties and Departments are responsible for their own information processing at various levels and requirements. This is similar to how Health and Safety responsibilities currently work in the University.

- Faculty Vice Presidents and Heads of Department have responsibility for the implementation of University information governance policies and procedures in their Departments and Services. The Vice-Presidents and heads of Faculty and Head of Departments should demonstrate visible commitment to information governance by:
  a) Ensuring that all staff undertake the mandatory training provided by the University.
  b) Ensuring that staff undertake specialised information governance training relevant to their roles (e.g. research data management).
  c) Ensuring that there are systems in the to maintain awareness of the information held and to ensure it is stored, used and shared only in accordance with University policies and procedures, maintaining an Information Asset Register.
  d) Providing sufficient resources for staff to be able to comply with University policies and procedures.
  e) Bringing to the attention of the University Secretary and the Data Protection Officer, any breach of statutory requirements which may be reportable or cannot be dealt with at Departmental or Service level and/or may have implications for the University more widely.
  f) Ensuring that staff co-operate fully with any information or information security audits authorised by IMG or Audit Committee.
  g) Ensuring students and staff are aware of the School or Service's procedures for secure handling of their personal data.
  h) Ensuring that University information governance policies and procedures are followed in any dealings, formal or informal, with third party individuals and organisations.

- Information Champions are appointed by Heads of Department to work on their behalf to ensure that policies are followed, mandatory training is completed, information asset registers are maintained and act as a local point of contact for incident reporting. A larger department with diverse areas of business e.g. Finance may have the need for more than one Information Champion, each with specialised knowledge of their respective areas. The Information Champion role should be considered a formal part of the individuals About The Job with the respective resource implications. They will be expected to undertake formal training relevant to the role.

- Information Asset Owners (IAOs) are responsible for the information they control. This is normally at a relatively local level e.g. a Primary Investigator defining how research data is managed for their specific project. IAOs must ensure that their information processing adheres to relevant policies and procedures for the University, their information asset, their department and any specialist constraints e.g. those demanded by an external research partner or funder.
  Senior Information Asset Owner (SIAO) have responsibilities to:

- Lead and foster a culture that values, protects and uses information for the success of the University and benefit of its stakeholders.
- Know what information the asset holds, and what information is transferred in and out of it and what systems it links to.
- Knows who has access to information assets and why; ensures their use is monitored and compliant with appropriate policies.
- Understands and addresses risks to the asset, providing assurance to the SIRO and ensure that any incidents are reported and managed following University guidelines.
- Ensure the information asset is fully used for its intended purpose.

An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Data Trustee
A Data Trustee is responsible for meeting quality requirements through the ongoing operational maintenance and management of data sources. They manage data and systems working with the Data Steward to agree changes. They have responsibilities to:

- Review, refine and improve business processes associated with data quality and maintenance on an ongoing basis.
- Define and undertake routine identification of data issues, including root cause analysis and report to the relevant Accountable Officer.
- Develop and maintain appropriate measures of data quality for specific datasets.
- Ensure policies for systems and the data they hold are clear and aligned across the University.
- Embed policies and protocols which promote the use of central systems to enable a ‘single source of truth’.

Information Users
Every member of the University has a responsibility for the information they are processing in their respective role.

- Information Users are people working day-to-day with information i.e. everyone.

- This includes all staff, students, visitors, 3rd parties (e.g. supplier and external research partners)

- Information users must ensure that they follow relevant policies and procedures defined by the IAO if working on a particular asset (e.g. a researcher on a project, a member of Income Office staff taking card payments) and any other relevant policies and procedures.

Information Users may find policies and procedures daunting but, in reality, many users will work with just a handful of general systems (e.g. email) and general assets (e.g. staff data) in a defined role which does not carry onerous or specialist policies and processes. Where there are specialisms (e.g. a researcher undertaking project work or a member of the Income Office taking card payments) then awareness of more bespoke policy and process requirement would form part of the induction, training and development of that individual. Information Users would generally approach their local Information Champion in the first instance for advice or signposting to more bespoke training or resources.