Roles and Responsibilities for Information Management Governance at the University of Sheffield

The principles of the structure align to accepted information management and information security approaches and to those implemented by other HEIs in the UK.

Figure 1. Structure for Information Management Governance. It is intended that 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

**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 which exist where further action is needed and make recommendations.

**IMG**
Accountability for recommending policy, monitoring and reporting on compliance and reporting risk has been delegated through UEB to the IMG. IMG, comprising representation from across the University, recommends strategy and policy to UEB and oversees delivery with support from the Information Management Operations Group and Data Governance Group. IMG is responsible for overseeing Information Governance policy and planning, developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the University and raising awareness of Information Governance.

**IMOOG**
The Information Management Operational Group (IMOOG) is the operational arm of IMG, tasked with the development and implementation of policies and processes on behalf of IMG.

- IMOOG comprises SIAO nominees to ensure that their responsibilities and requirements are considered
- IMOOG also comprises IG Leads in specialist domains such as Information Security, Records Management, Research Data Management and Data Protection
- In reality the standing membership of IMOOG is rationalised to avoid an excess number of people with overlapping interests; additional working groups serving a ‘task and finish’ function will be formed from respective expertise across the University when required.

**Data Governance Group**
The Data Governance Groups terms of reference include:

- Overseeing the University's Data Governance Structure to ensure that it remains current and fit for purpose and is consistent across all systems
- Overseeing the development of a defined and consistent set of procedures for data quality, and a plan to execute those procedures by relevant Professional Services
- Establishing task and finish groups as required to develop specific aspects of data governance
- Developing a communications plan to promote understanding of data governance and the benefits of implementing good data governance practices

**Compliance and Reporting**

**University Secretary**
The University Secretary is responsible to the President and Vice-Chancellor on a delegated basis for the general oversight of compliance and risk 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. As Chair of IMG, the University Secretary has responsibility for ensuring policies and procedures are proposed and implemented, that mechanisms are established to monitor their effectiveness and to report on compliance and risk. Faculties and Departments remain responsible for compliance with data protection law and must be able to demonstrate compliance.

**Data Protection Officer**
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.

**COO**
The COO is the named Senior Information Risk Owner (SIRO) in UEB, accountable for all information 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. Owns the University's information incident management framework.

**Faculties and Departments**
Faculties and Departments are generally responsible for their own information processing at various levels and requirement.

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 FVP and Head of Departments should demonstrate visible commitment to good information governance by:

- Ensuring that all staff undertake the mandatory training provided by the University.
- Ensuring that staff undertake specialised information governance training relevant to their roles (e.g. research data management).
- 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.
- Providing sufficient resources for staff to be able to comply with University policies and procedures.
- 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.
- Ensuring that staff co-operate fully with any information or information security audits authorised by IMG or Audit Committee.
- Ensuring students and staff are aware of the School or Service’s procedures for secure handling of their personal data.
- Ensuring that University information governance policies and procedures are followed in any dealings, formal or informal, with third party individuals and organisations.

Information Champions 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 Guardian 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.

**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 Guardian in the first instance for advice or signposting to more bespoke training or resources.