Information Governance Framework

Brunel University London

Document Properties

Author

Head of Privacy

Executive Sponsor

University Secretary and Legal Counsel

Responsible Officer

Head of Privacy

Version Control

Version	Author	Comments	Date
0.1	Head of Privacy	Initial Draft for comment	20/05/ 2024
0.2	Head of Privacy	Amendments following consultation	04/06/2024
0.3	Head of Privacy & Head of Cyber Resiliance	Amendments made actions identified in IAC. Once corrections made IAC happy for the Framework to published.	09/08/2024
1.0	Published version		09/08/20

Contents

Executive Summary

Information is a vital asset for all aspects of BUL’s operation and for the efficient management of Brunel’s resources. As well as protecting and providing the rights of access to public and personal information, it plays an increasingly strategic role in the way in which Brunel is regulated and held accountable by external bodies. Insight and intelligence gathering from our data is key to understanding our institutional position and performance. It plays a key role in the management and governance of Brunel and its future planning.

As the steward of this information and data, Brunel has the responsibility to ensure that its information is managed, secure and used effectively while it is within our environment. An Information Governance framework is a set of rules, processes, and responsibilities setting out how we collect, organise, store, and use our data, leading to efficient decision making regarding the management of information through its lifecycle.

Introduction

Information is a vital asset for all aspects of Brunel University London's (BUL) operation and for the efficient management of BUL's resources. As well as protecting and providing the rights of access to public and personal information, it plays an increasingly strategic role in the way in which BUL is regulated and held accountable by external bodies. Insight and intelligence gathering from our data is key to understanding our institutional position and performance. It plays a key role in the management and governance of BUL and its future planning

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 BUL. It describes how information is to be governed as a vital business asset which is essential to help meet BUL's business, accountability, legal and regulatory requirements. 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 BUL.

Information is a key asset for BUL and as such the IG Framework requires cooperation and commitment from all relevant stakeholders.
The protection of personal data and how organisations ensure that an individual's right to privacy is respected has become a significant strategic objective of all businesses including those within the Higher Education sector in recent years.

Purpose

This Framework establishes and sets out the roles and responsibilities associated with the management of BUL's information, data and systems assets.

Scope

The IG Framework applies to all employees, regardless of contract type; consultants; contractors; research students, other relevant parties processing or managing information on BUL's behalf.

The IG Framework applies to all information processed by or on behalf of BUL, (whether hard copy or digital) including, but not limited to, the provision of:

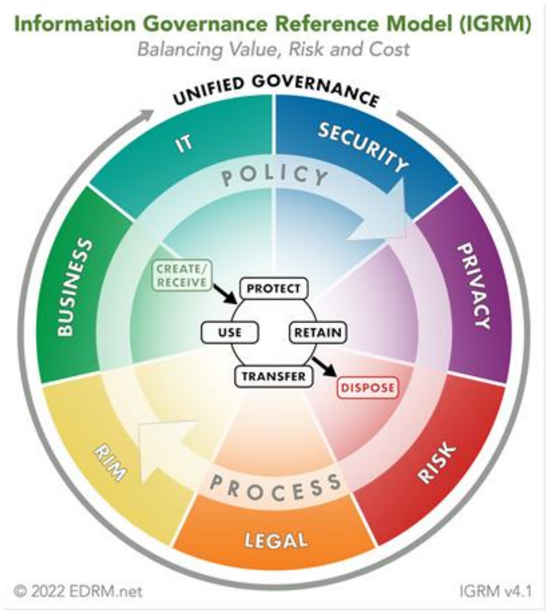
- teaching and education data
- research data
- student and alumni data
- staff data
- enterprise and community engagement data
- business and commercial activity data

- internal and external reporting data
- finance data
- space and asset data

Definitions

Data are facts and statistics collected together for reference or analysis. When data are processed, organised, structured or presented in a way that gives it context and therefore makes it more useful, it is called information. In the context of this document and BUL's Information Governance Framework, the terms data and information can be used interchangeably.

Information Governance looks at the whole organisation. Using the IG Reference Model key stakeholders can understand their role in managing information effectively and how effective management can only be achieved through collaboration across our organisation.



The IGRM has information at its heart and reflects the lifecycle of information starting at its creation/receipt and shows the linkage between value and the duty to manage information assets. The basic principles of using information, protection, retention, transferring (or sharing) with the final act of disposal is at the heart of effective management of information and data management. Wrapped around this are the supporting elements of policy and process – and each segment identifies key business areas that impact and influence how data is managed. It also recognises that for data to be managed efficiently, it is essential to link specific responsibilities and business value to information assets.

As each data or information asset is assessed, elements of the reference model balance themselves out according to the value placed on it. For example, a data asset that contains contact information and email address for many staff/students. We must consider all the elements:

Business	We must have a way to contact our staff/students easily and efficiently to deliver our business.
Information Technology (IT)	We provide tools to ensure that easy contact and communications can be delivered, that are maintained and updated.
Security	We provide the secure environment in which our email address book is secure and protected from corruption and malicious actions.
Privacy	We ensure that we have the right legal basis for use and can ensure that the rights of the individual are protected.

Risk	We ensure that all risks to the management of information are identified and appropriate and relevant mitigations are in place
Legal	We ensure that any legal obligations are met
RIM	We ensure that appropriated Records and Information Processes are in place, meeting both our public record and information rights obligations.

With these considerations BUL will establish and maintain policies and procedures for the effective and secure management of its information assets ensuring it is properly held, obtained, recorded, used and shared ensuring compliance, lessening risk, increasing business efficiencies, creating a better working environment and securing the data of its staff and stakeholders.

INFORMATION GOVERNANCE FRAMEWORK

Within the context of this Framework BUL will establish and embed policies and processes to meet the following aims (see also Annex A for an overview):

- Information is created and processed in compliance with legislation and to meet business requirements
- Information is reliable and trustworthy and vital records are identified
- Information, data and records can be easily identified and accessed by the appropriate people when necessary
- Information is kept in accordance with business and legal requirements and disposed of when necessary
- Information of enduring historical value is preserved permanently for future generations
- Staff understand value of IG and the skills to implement best practice
- Build awareness of information as an asset into the development of systems and processes ensuring that it is protected and securely managed

Embedding good Information Governance practices within BUL will:

- Contribute to BUL's strategic plan by supporting teaching, research, enterprise and partnerships and contributing to its digital and people development
- Improve the management of information and records
- Ensure compliance with legislation and improve business efficiencies
- Establish clear policies, responsibilities, and ownership in relation to data protection, information access, information management and information security.
- Reduce financial, operational, legal and reputational risk

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

General

BUL will establish and maintain policies, standards and procedures for the effective and secure management of its information assets.

BUL will accurately identify and classify information to ensure that it is handled and shared appropriately, in line with the BUL Information Classification Procedure. The classification of BUL's data will be managed using our Microsoft 365 environment and the security classification set out in the established Information Classification Procedure. This will be included as an action in the Digital Strategy as it will be carried out in partnership with IS.

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.

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

Regulatory Compliance

BUL will implement policies to assist compliance with the Freedom of Information Act and the Environmental Information Regulations.

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

BUL will maintain Records of Processing Activities (RoPA) in accordance with Article 30 of the UK GDPR.

> The RoPA logs the business areas and associated data across the professional services body of the University. It shows how data is linked to systems, processes, legal basis of processing, contracts, DPIA's and retention criteria. The output of the RoPA will be linked to an information asset register being developed by IS and will support the Privacy Team in responding quickly to information requests as it will enable quicker identification of data sources. The approach to develop the RoPA will be to work with the Information Champions and other key stakeholders across BUL to build a robust, managed record.

Mandatory Information Security and Data Protection training must be undertaken by all staff on an annual basis.

Targeted training on specific subjects relating to information governance will be developed in response to specialist needs as well as the Information Champion role. A training needs analysis will be developed working with key stakeholders such as HR, IS and Records, Archives & Special Collections.

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

Key associated policies:

- Data Protection and Information Access Policy
- Freedom of Information (and EIRs) Policy
- Publication Scheme
- Staff guidance on Data Protection and Freedom of Information Act (FOIA)
- Guidance on Data Protection Impact Assessments
- Identity and Access Management Policy
- Information Governance Training Needs Assessment and Training Plan
- Privacy Notices
- Incident/Breach reporting procedure and guidance
- Records Management Policy
- Records Retention and Disposal Policy
- Information Compliance: handling staff personal data
- Information Compliance: handling student personal data
- IT Acceptable Use Policy

Management and Security

BUL will maintain policies, procedures and standard operating procedures (SOPs) for the effective and secure management of its information assets.

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

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

Key roles, as defined in the section on Roles, Responsibilities and Reporting will work together to ensure appropriate accountability and scrutiny of Information Governance across BUL via a formal committee reporting structure (see Annex B).

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

BUL 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.

Associated key policies:

- Information Security Policy
- Bring Your Own Device Policy
- Identity and Access Management Policy
- Information Classification Policy
- Password Policy
- Threat & Vulnerability Mngt Policy
- System Security Policy
- Security Awareness Policy
- Supply Chain Security Policy
- Security Incident Mngt Policy
- User Endpoint Security Policy
- Physical Security Policy
- CCTV and Surveillance Policy

Roles, Responsibilities and Reporting

The key roles and related responsibilities are set out below (see also Annex B). Full role descriptions will also be created where needed.

Senior Information Risk Owner (SIRO)

The SIRO Role is to:

- take the lead for managing information risks, including maintaining and reviewing an Information risk register, including chairing the Information Assurance Committee (IAC)
- oversight of security, incident and risk management and reporting.
- escalate and advise on any significant issues affecting Information Governance, risk and security to senior management.
- The SIRO shall receive training as necessary to ensure they remain effective in their role.

Data Protection Officer (DPO)

As a public body, BUL is required to appoint a DPO in accordance with Articles 37 –

39 of the UK GDPR. The DPO 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.
- To co-operate with and be the first point of contact for supervisory authorities; to engage with individuals whose data is processed by BUL.
- The DPO shall receive training as necessary to ensure they remain effective in their role.
- 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 Senior Management at any time.

Information Asset Owner (IAO)

The most senior member of staff of a Directorate or College, 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.

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.

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

Information Asset Manager (IAM)

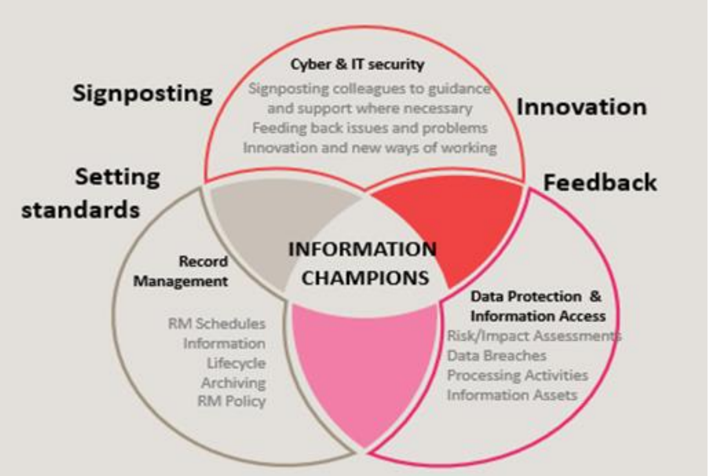
Designated by, and responsible to, the relevant IAO, Information Asset Managers are individuals with operational responsibility for specific information assets. They are business users with expert knowledge of business processes and how data is used within those processes.

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.

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

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

Information Champions (IC) (Previously Data Protection Champions)



An Information Champion's role is to embed good practice and enable an information culture in which staff and students are aware of sources of information relating to:

- data protection
- cyber and information security
- digital skills and literacy
- records management
- archives
- training

and how the elements illustrated by the IGRM of robust Information Governance good practice can be applied to their work.

An IC is an advocate for information governance issues, providing a central point of contact and signposting colleagues to further help and support, relevant policies and procedures and provide support in recognising potential issues that may need to be escalated

An IC will ensure that best practice, including new guidelines and ways of working, are circulated, understood and implemented locally, through departmental meetings and other routes.

An IC will be able to assist their colleagues in identifying and reporting Information Governance issues and risks from project development through to business as usual.

There will be an ***Information Champions Network*** which will enable a culture of sharing and support between and with colleagues. They will contribute to the ***Information Assurance Working Group*** established to provide a forum in which they can share ideas, get involved in the development of processes and procedures and contribute to standards for operating, feedback their local teams' views, opinions and suggestions, and provide the opportunity to be involved in new innovations in the way we work.

Information champions will receive additional training and support on understanding Data Protection principles and good practice, IT and Information Security and Records Management. A training needs analysis will be developed working with key stakeholders such as HR, IS and Records, Archives & Special Collections.

Information Assurance Committee (IAC)

The IAC comprises key roles relating to Information and Data Governance as set out in its Terms of Reference and has oversight and responsibility for matters relating to managing Information

Governance, including responsibility for policies, frameworks, risk analysis and strategic initiatives to facilitate best practice across BUL. The Information Assurance Group reports to the Executive Board.

All individuals and organisations who process information on behalf of BUL have a responsibility, under the necessary agreements, to comply with information governance framework and its policies, including data protection, access to information and information security procedures. All are responsible for undertaking mandatory Information Governance online training.

Reporting

The Executive Board receives risk assurance from the Information Governance Committee and oversees and monitors the application of effective information risk management including University-wide compliance with Information Governance, Data Protection & Information Access and Cyber & Information Security policies and initiatives.

Associated Policies and Procedures

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

External Legislation

BUL'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:

1. UK General Data Protection Regulation (GDPR) / Data Protection Act 2018 (DPA18)
2. Human Rights Act 1998 (HRA98)
3. Freedom of Information Act 2000 (FOI) / Environmental Information Regulations 2004 (EIR)
4. Computer Misuse Act 1990
5. Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
6. Copyright, Designs and Patents Act 1988
7. Malicious Communications Act 1988
8. Intellectual Property Act 2014
9. Investigatory Powers Act 2016
10. Regulation of Investigatory Powers Act 2000
11. Equalities Act 2010
12. Limitation Act 1980

Regulators

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

- ICO
- Office for Students
- Higher Education Statistics Agency
- Department for Education

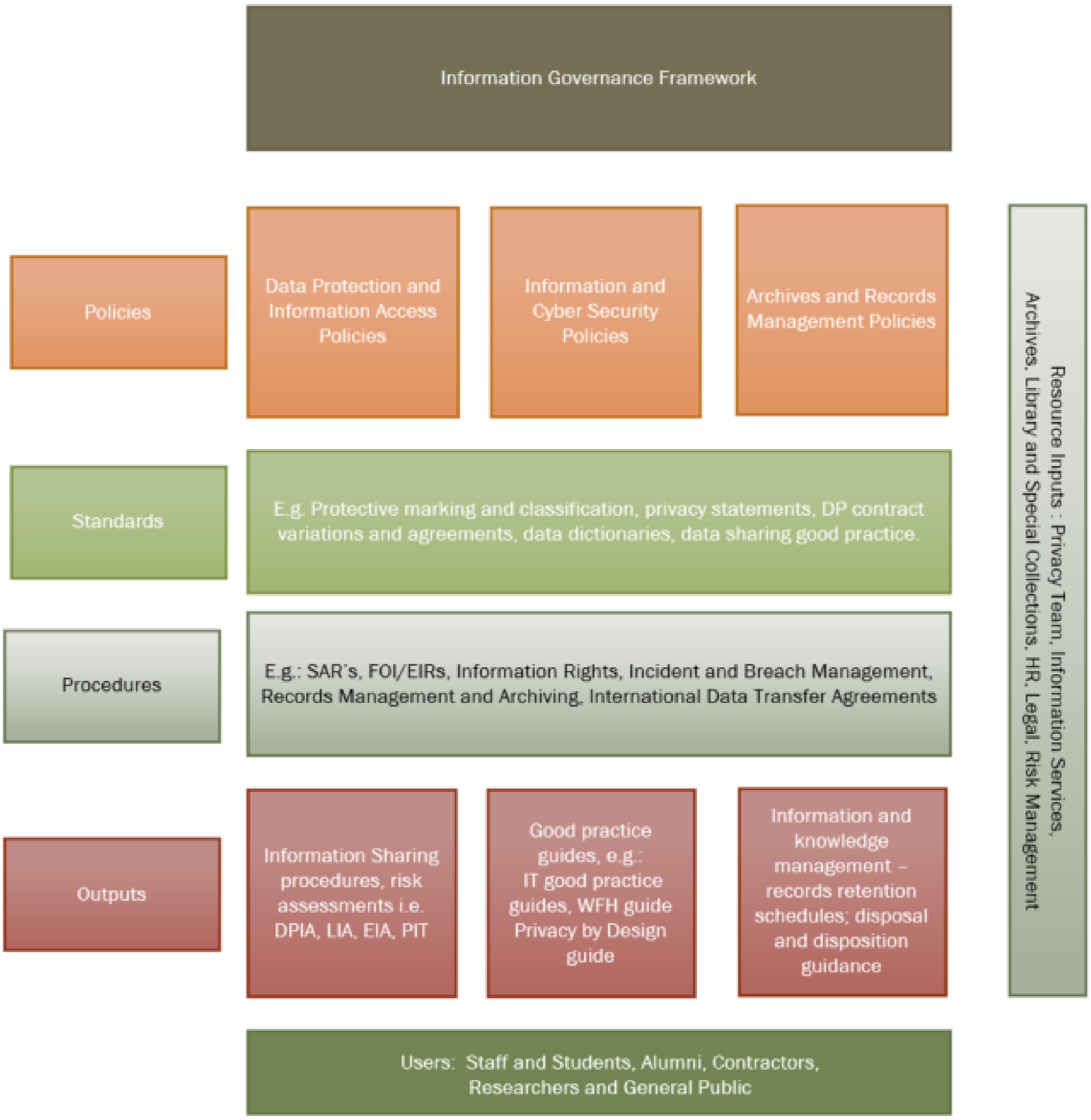
Review, Approval & Publication

The IG Framework will be reviewed, at a minimum, every two years. The IAC is responsible for such review. The IG Framework will require approval by the Executive Board and will then be published

Annexes

Annex A: Information Governance Framework
Annex B: Roles and responsibilities for the management and governance of information assets
Annex C: Key Policies

Annex A: The Information Governance Framework Documentation



Information Governance Framework

Policies

Data Protection and Information Access Policies

Information and Cyber Security Policies

Archives and Records Management Policies

Standards

E.g. Protective marking and classification, privacy statements, DP contract variations and agreements, data dictionaries, data sharing good practice.

Procedures

E.g.: SAR's, FOI/EIRs, Information Rights, Incident and Breach Management, Records Management and Archiving, International Data Transfer Agreements

Outputs

Information Sharing procedures, risk assessments i.e. DPIA, LIA, EIA, PIT

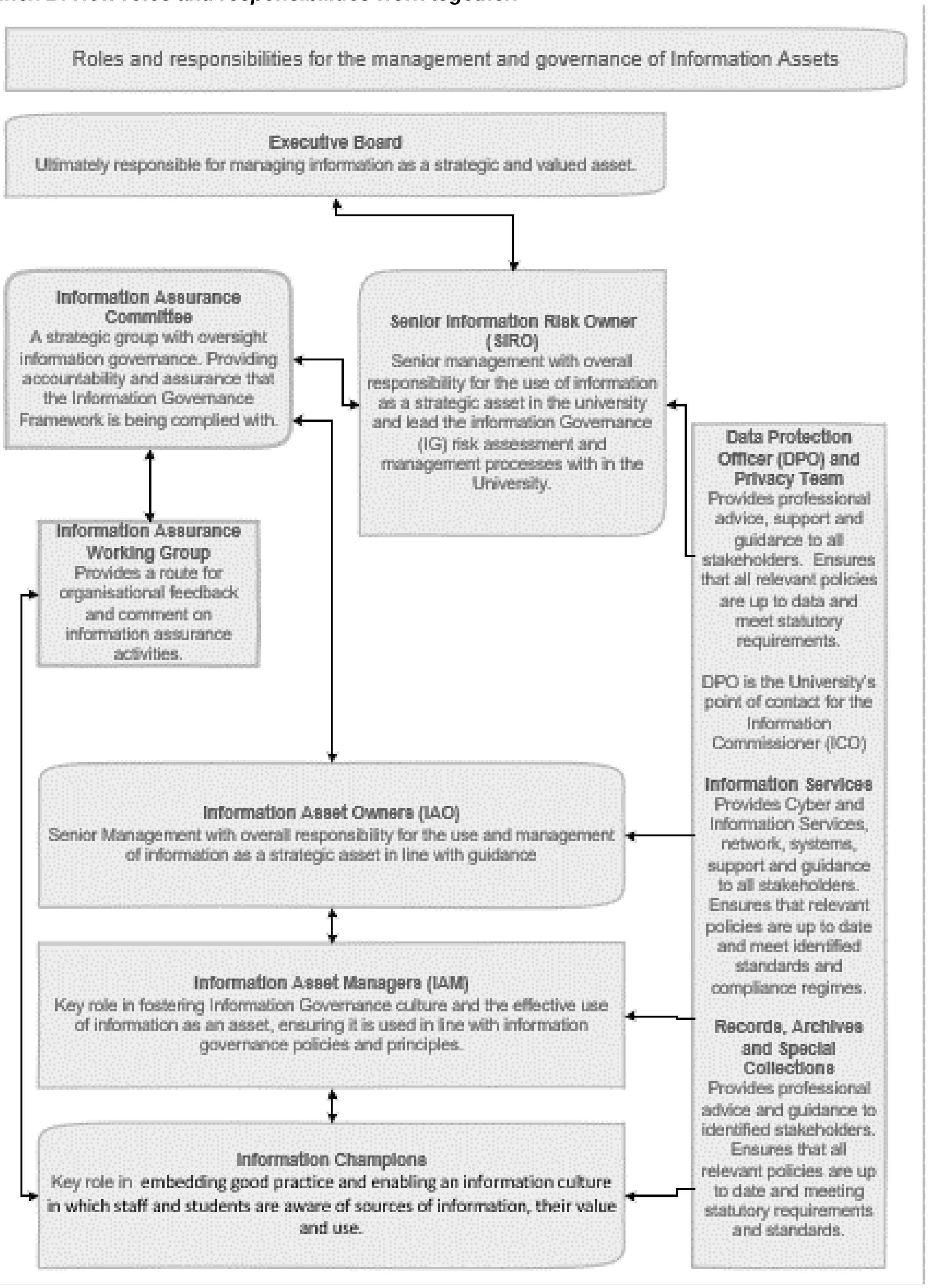
Good practice guides, e.g.: IT good practice guides, WFH guide Privacy by Design guide

Information and knowledge management – records retention schedules; disposal and disposition guidance

Users: Staff and Students, Alumni, Contractors, Researchers and General Public

Resource Inputs : Privacy Team, Information Services, Archives, Library and Special Collections, HR, Legal, Risk Management

Annex B: How roles and responsibilities work together.



Roles and responsibilities for the management and governance of Information Assets

Executive Board
Ultimately responsible for managing information as a strategic and valued asset.

Information Assurance Committee
A strategic group with oversight information governance. Providing accountability and assurance that the Information Governance Framework is being complied with.

Senior Information Risk Owner (SIRO)
Senior management with overall responsibility for the use of information as a strategic asset in the university and lead the information Governance (IG) risk assessment and management processes with in the University.

Information Assurance Working Group
Provides a route for organisational feedback and comment on information assurance activities.

Data Protection Officer (DPO) and Privacy Team
Provides professional advice, support and guidance to all stakeholders. Ensures that all relevant policies are up to data and meet statutory requirements.

DPO is the University's point of contact for the Information Commissioner (ICO)

Information Services
Provides Cyber and Information Services, network, systems, support and guidance to all stakeholders. Ensures that relevant policies are up to date and meet identified standards and compliance regimes.

Records, Archives and Special Collections
Provides professional advice and guidance to identified stakeholders. Ensures that all relevant policies are up to date and meeting statutory requirements and standards.

Information Asset Owners (IAO)
Senior Management with overall responsibility for the use and management of information as a strategic asset in line with guidance

Information Asset Managers (IAM)
Key role in fostering Information Governance culture and the effective use of information as an asset, ensuring it is used in line with information governance policies and principles.

Information Champions
Key role in embedding good practice and enabling an information culture in which staff and students are aware of sources of information, their value and use.

Annex C: Key Policies

Policy	Owner/Lead
Bring Your Own Device Policy	IS
CCTV and Surveillance Policy	Security and Campus Support
Data Handling Policy	Privacy Team
Data Protection and Information Access Policy	Privacy Team
Freedom of Information (and EIRs) Policy	Privacy Team
Guidance on Data Protection Impact Assessments	Privacy Team
Identity & Access Management Policy	IS
Incident/Breach reporting procedure and guidance	Privacy Team
Information Classification Policy	IS & Privacy
Information Governance Training Needs Assessment and Training Plan	IS; Privacy Team; Records, Archives & Special Collections
Information Security Policy (Top Level)	IS
IT Acceptable Usable Policy	IS
Password Policy	IS
Physical Security Policy	IS
Privacy Notices	Privacy Team
Publication Scheme	Privacy Team
Records Management Policy	Records, Archives & Special Collections
Records Retention and Disposal Policy	Records, Archives & Special Collections
Security Awareness Policy	IS
Security Incident Mngt Policy	IS
Staff guidance on Data Protection and Freedom of Information Act (FOIA)	Privacy Team
Supply Chain Security Policy	IS
System Security Policy	IS
Threat & Vulnerability Mngt Policy	IS
User Endpoint Security Policy	IS