



Information Governance Framework

Brunel University London

Document Properties

Author

Head of Privacy

Executive Sponsor

University Secretary and Legal Counsel

Responsible Officer

Head of Privacy/Data Protection Officer

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 Resilience	Amendments made following actions identified by IAC. Once corrections were made, IAC confirmed the Framework was ready for publication.	09/08/2024
1.0	Published version		09/08/2024
1.1	Head of Privacy & Head of Information Security	Amendments made to policies, functions and the annexes to bring them up to date and ready for additions later this year.	02/07/2026

Contents

Executive Summary	4
Introduction	5
Purpose	5
Scope	5
Definitions	6
INFORMATION GOVERNANCE FRAMEWORK	7
General	7
Regulatory Compliance	8
Information rights	9
Artificial intelligence and automated decision-making	9
Third-party processing and data sharing	9
Management and Security	10
Retention, disposal and legal holds	10
Research data governance	10
Cyber resilience and business continuity	11
Roles, Responsibilities and Reporting	11
<i>Senior Information Risk Owner (SIRO)</i>	11
<i>Data Protection Officer (DPO)</i>	12
<i>Information Asset Owner (IAO)</i>	12
<i>Information Asset Manager (IAM)</i>	12
<i>Business Service Manager (BSO)</i>	12
<i>Information Champions</i>	13
<i>Information Assurance Committee (IAC)</i>	14
Reporting	14
Monitoring and Assurance	14
Implementation and Improvement Plan	14
Information Governance Maturity Model	15
Associated Policies and Procedures	16
External Legislation	16
Regulators	16
Review, Approval & Publication	16
Annexes	17
<i>Annex A: The Information Governance Framework Documentation</i>	18
<i>Annex B: How roles and responsibilities work together.</i>	19
<i>Annex C: Key Policies</i>	20

Executive Summary

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

This Information Governance Framework (the 'IG Framework') and its associated policies aim 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 BUoL. It describes how information is to be governed as a vital business asset which is essential to help meet BUoL'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 BUoL.

Information is a key asset for BUoL 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 BUoL'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 BUoL's behalf.

The IG Framework applies to all information processed by or on behalf of BUoL, (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 BUoL'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 appropriate records and information processes are in place, meeting both our public records and information rights obligations.

With these considerations BUoL 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 BUoL 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 the value of IG and have 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 BUoL will:

- Contribute to BUoL'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

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

General

BUoL will establish and maintain policies, standards and procedures for the effective and secure

management of its information assets.

BUoL will accurately identify and classify information to ensure that it is handled and shared appropriately, in line with the BUoL Information Classification Procedure. The classification of BUoL'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 BUoL will ensure that Information Governance will be considered at all stages of processing.

Regulatory Compliance

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

BUoL will implement policies to assist compliance with the Data Protection Act 2018 and UK General Data Protection Regulation.

BUoL 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, DPIAs 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 developing the RoPA will be to work with the Information Champions and other key stakeholders across BUoL 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.

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

Information rights

BUoL will maintain clear processes for managing statutory information rights requests, including subject access requests, requests for rectification, erasure, restriction, objection and data portability, as well as requests under the Freedom of Information Act and Environmental Information Regulations. These processes will support timely identification, retrieval, review and disclosure of information, ensure appropriate escalation where complex or sensitive issues arise, and enable compliance with statutory deadlines.

Artificial intelligence and automated decision-making

Where BUoL uses artificial intelligence, automated decision-making or algorithmic tools to support teaching, research, administration or decision-making, appropriate governance controls must be applied. This includes consideration of lawful basis, fairness, transparency, accuracy, bias, human oversight, security, records management, supplier assurance and the rights of individuals. High-risk uses must be assessed through appropriate risk assessment processes, including Data Protection Impact Assessments where required, and must be supported by clear privacy information and documented accountability.

Third-party processing and data sharing

BUoL will ensure that information shared with, or processed by, external organisations is governed by appropriate contracts, data processing agreements, data sharing agreements or other documented arrangements. These arrangements must set out the purpose of the sharing or processing, the responsibilities of each party, security requirements, retention and disposal arrangements, audit or assurance expectations, and any international transfer requirements. Supplier and partner arrangements must be reviewed proportionately to the level of risk and sensitivity of the information involved.

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
- Handling of staff and student data Guidance
- IT Acceptable Usage Policy

Management and Security

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

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

BUoL 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 BUoL via a formal committee reporting structure (see Annex B).

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

BUoL 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.

Retention, disposal and legal holds

BUoL will manage information in line with approved retention schedules so that records are kept for as long as required for business, legal, regulatory, audit and historical purposes and are securely disposed of when no longer required. Where information is required for litigation, investigation, audit, complaint handling or regulatory review, appropriate legal hold or preservation arrangements must be applied before disposal takes place.

Research data governance

Research data must be managed in accordance with applicable legal, ethical, contractual, funder and institutional requirements. This includes appropriate consideration of research ethics approvals, data management plans, consent and transparency, special category data, anonymisation or pseudonymisation, secure storage, controlled sharing, retention, archiving and reuse. Research involving personal data must be supported by proportionate privacy and security controls throughout the research lifecycle.

Cyber resilience and business continuity

Information Governance supports cyber resilience and business continuity by ensuring that critical information assets, systems and records are identified, protected, recoverable and subject to appropriate access controls. Business continuity and incident response arrangements should consider the availability, integrity and confidentiality of key information assets, including backup, restoration, continuity of access, incident escalation and post-incident review.

Associated key policies:

- IT Acceptable Usage Policy
- Bring Your Own Device Policy
- Identity and Access Management Policy
- Information Classification Policy
- Password Policy
- Threat and Vulnerability Management Policy
- System Security Policy
- Information Security Awareness Policy
- Supply Chain Risk Management Policy
- Information Security Incident Management Policy
- User Endpoint Security Policy
- Network 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 and 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, BUoL 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 BUoL.
- 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 information Asset Owner is a member of the Senior Management with overall accountability for the information Assets within their business. They sit on the Executive Board and provide oversight and strategic direction for asset use and have oversight of key risks.

Information Asset Manager (IAM)

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

IAMs 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.

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

Business Service Manager (BSO)

Designated by, and responsible to, the relevant IAM, Business Service 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 BSO's role is to maintain Information Asset Risks in their area, raise any information management issues and risks with the IAM, monitor completion of mandatory Information Security training and ensure staff are aware of best practice and compliance requirements.

The BSO's may nominate individuals to provide administrative support as necessary.

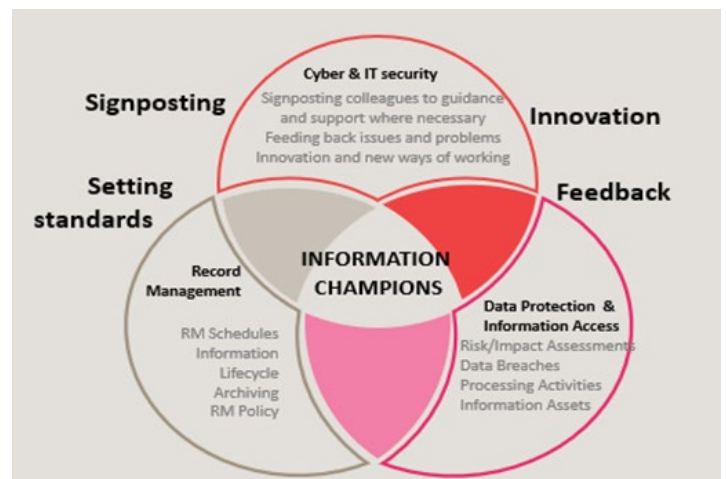
The BSO's and their nominees shall receive training as necessary to assist them in their role.

Information 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, signposting colleagues to further help and support, relevant policies and procedures, and providing 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, is 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 colleagues. The Network will contribute to the ***Information Assurance Working Group***, established to provide a forum in which Information Champions can share ideas, get involved in the development of processes and procedures, contribute to operating standards, feed back their

local teams' views, opinions and suggestions, and be involved in new ways of working.

Information Champions will receive additional training and support on data protection principles, 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 information governance, including responsibility for policies, frameworks, risk analysis and strategic initiatives to facilitate best practice across BUoL. The Information Assurance Committee reports to the Executive Board.

All individuals and organisations who process information on behalf of BUoL have a responsibility, under the necessary agreements, to comply with the 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 Assurance Committee and oversees and monitors the application of effective information risk management, including University-wide compliance with Information Governance, Data Protection and Information Access, and Cyber and Information Security policies and initiatives.

Monitoring and Assurance

BUoL will monitor the effectiveness of this Framework through regular reporting to the Information Assurance Committee and, where appropriate, onward reporting to senior management. Assurance will be drawn from policy compliance, risk reporting, audit outcomes, training completion, incident trends, information rights performance, DPIA activity, Records of Processing Activities coverage, Information Asset Register completion, retention and disposal activity, supplier assurance and progress against agreed improvement actions.

The IAC will use this assurance to identify areas of good practice, emerging risks, overdue actions and areas requiring additional support or escalation. Key measures may include completion of mandatory training, number and severity of information incidents, timeliness of statutory information rights responses, completion of DPIAs, RoPA and Information Asset Register coverage, policy review status, audit findings and closure of agreed actions.

Implementation and Improvement Plan

The implementation of this Framework will be supported by an improvement plan agreed and monitored by the Information Assurance Committee. Priority actions will include maintaining and improving the Records of Processing Activities, developing Information Asset Registers, embedding the Information Champions Network, strengthening information classification, improving retention and disposal practice, supporting DPIA completion, developing targeted training and improving assurance over third-party processing and data sharing.

Progress against the improvement plan will be reviewed regularly by IAC, with significant risks, delays or resource issues escalated through the agreed governance route. The plan should identify the lead owner, timescale, dependency, intended outcome and assurance evidence for each action.

Information Governance Maturity Model

BUoL will use an Information Governance maturity model to assess the extent to which good practice is defined, implemented, embedded and evidenced across the University. The model will support proportionate improvement planning, provide a common language for discussing progress, and help IAC identify priority areas for assurance, support and escalation.

The maturity model is intended to be used as a practical assurance tool rather than a compliance score. It should be applied to key areas of information governance, including Records of Processing Activities, Information Asset Registers, information classification, retention and disposal, information rights, DPIAs, data sharing, third-party processing, incident management, training and awareness, AI and automated decision-making governance, and cyber and information security alignment.

Level	Maturity stage	Description
1	Initial	Activity is informal, inconsistent or reactive. Roles, processes and evidence may be unclear or dependent on individual knowledge.
2	Defined	Policies, procedures, roles and responsibilities are documented, but implementation may be inconsistent across areas.
3	Implemented	Processes are in regular use, ownership is understood, and evidence is available to show that requirements are being applied in practice.
4	Measured	Performance is monitored through agreed measures, assurance reporting, audit findings, risk reporting and improvement actions.
5	Optimised	Good practice is embedded, continuously improved and supported by reliable evidence, benchmarking, lessons learned and proactive risk management.

Maturity assessments should be reviewed periodically by IAC and used to inform the Information Governance improvement plan. Where a key area is assessed at a lower maturity level, the improvement plan should identify the action required, accountable owner, timescale, dependency, target maturity level and evidence needed to demonstrate progress.

Associated Policies and Procedures

This Framework sets out the high-level principles and policies for Information Governance across BUoL. 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

BUoL'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 (UK GDPR) / Data Protection Act 2018 (DPA 2018)
2. Data Use and Access Act (DUAA) 2025
3. Human Rights Act 1998 (HRA 1998)
4. Freedom of Information Act 2000 (FOIA) / Environmental Information Regulations 2004 (EIR)
5. Computer Misuse Act 1990
6. Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
7. Copyright, Designs and Patents Act 1988
8. Malicious Communications Act 1988
9. Intellectual Property Act 2014
10. Investigatory Powers Act 2016
11. Regulation of Investigatory Powers Act 2000
12. Equality Act 2010
13. Limitation Act 1980

Regulators

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

- The Information Commission
- 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 this

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

The Information Governance Framework is supported by a hierarchy of policies, procedures, standards, guidance and assurance records. Together these documents explain what BUoL must do, who is responsible, how requirements should be applied in practice and how compliance will be monitored.

Document type	Purpose
Framework	Sets the overall principles, governance structure, roles, responsibilities and assurance approach for information governance across BUoL.
Policies	Set mandatory institutional requirements for data protection, information access, records management, information security, classification, acceptable use and related areas.
Procedures and SOPs	Explain how staff should carry out specific activities, such as responding to information rights requests, reporting incidents, completing DPIAs, applying retention rules or classifying information.
Guidance and training (outputs)	Provides practical support for staff, Information Champions, IAOs and IAMs to apply good information governance in day-to-day work.
Registers and assurance records (outputs)	Evidence compliance and support oversight, including Records of Processing Activities, Information Asset Registers, DPIAs, incident logs, risk registers, policy review records, training reports and audit actions.

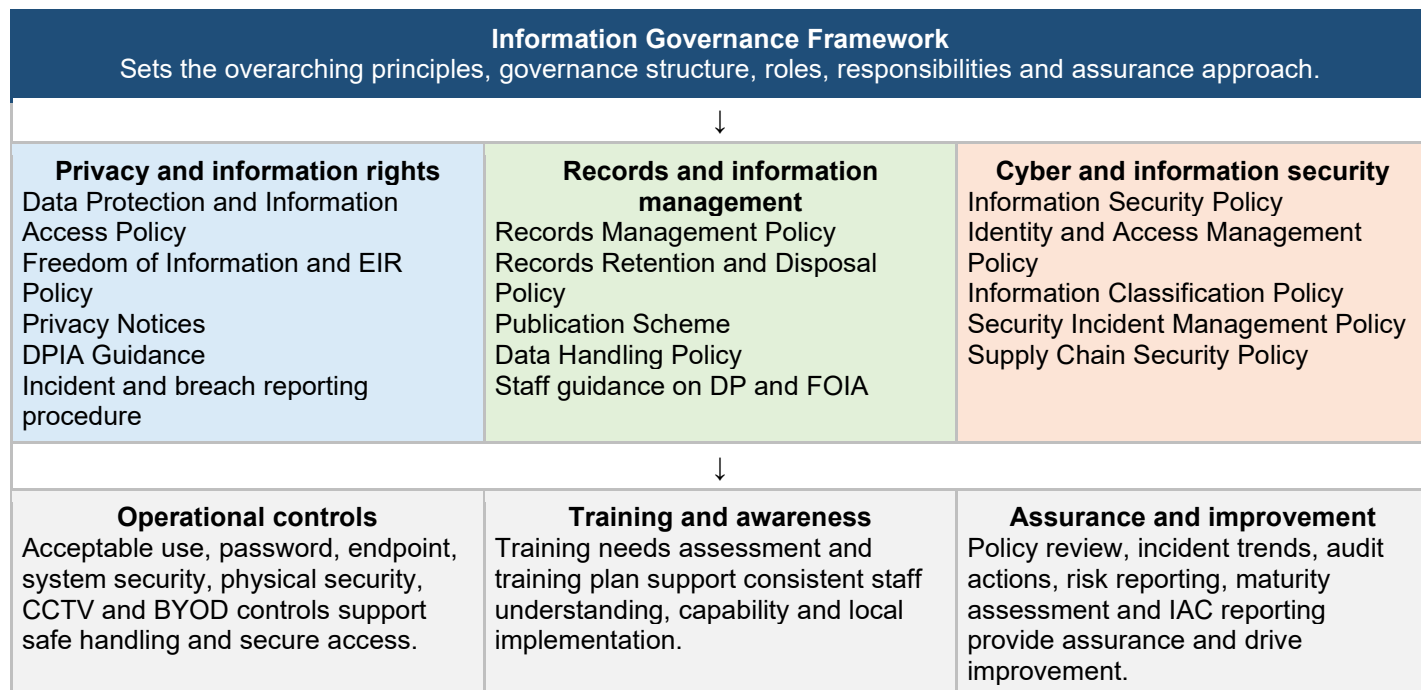
Annex B: How roles and responsibilities work together.

Effective information governance depends on clear ownership, practical local support and a defined route for assurance and escalation. The table below summarises how the key roles and groups work together.

Executive Board		
Receives assurance and oversees institutional information risk, compliance and improvement.		
↑ escalation and assurance reporting		
Data Protection Officer Provides independent advice on data protection compliance, DPIAs, information rights and ICO engagement. Escalation: serious data protection concerns may be reported to the highest level of the organisation.	Information Assurance Committee Oversees the Framework, reviews risks, monitors assurance and drives improvement activity. Escalation: significant risks and assurance findings are reported through the agreed senior governance route.	Senior Information Risk Owner Owns senior information risk oversight, chairs IAC and escalates significant information risks to senior management.
↑ specialist assurance, advice, evidence and escalation		
Digital Services Provides technical controls, secure systems, access management, cyber resilience, system security, supplier/security assurance and support for digital information assets. Works with: IAC, SIRO, IAOs, IAMs, Business Service Owners and Information Champions.	Archives and Records Management Provides specialist advice and assurance on records management, retention, disposal, legal holds, information lifecycle management, archives and preservation. Works with: IAC, IAOs, IAMs, Business Service Owners and Information Champions.	
↑ risks, issues, assurance evidence and improvement actions		
Information Asset Owners Accountable for information assets, risks and controls within their area to the Executive Board		
↑ local issues, asset risks, training needs and control updates		
Information Asset Managers Maintain local Information Assets and support the management of information risks and controls. for reporting risks and assurance issues to the SIRO through IAC or agreed management routes.		
↑ operational questions, process issues, asset updates and local support needs		
Business Service Owners Support local information asset management and operational control of information risks within specific services and processes.	Information Champions Promote good practice, signpost colleagues to guidance and feed issues, feedback and improvement ideas into the Information Champions Network and IAC working arrangements.	
↑ day-to-day questions, local feedback, incidents, risks and improvement needs		
All staff, students, contractors and third parties processing BUoL information Apply policies and procedures, complete mandatory training, protect information, report incidents and raise concerns through local or specialist routes.		

Annex C: Key Policies

The diagram below shows how the key policies in Annex C support the Information Governance Framework and how they group into the main areas of accountability, control and assurance.



Consolidated key policies and guidance

No.	Policy / guidance	Category
1	Bring Your Own Device Policy	Cyber and information security
2	CCTV and Surveillance Policy	Physical and surveillance security
3	Data Protection and Information Access Policy	Privacy and information rights
4	Freedom of Information (and EIRs) Policy	Privacy and information rights
5	Guidance on Data Protection Impact Assessments	Privacy and information rights
6	Handling of staff and student data Guidance	Data handling guidance
7	Identity and Access Management Policy	Cyber and information security
8	Incident/Breach reporting procedure and guidance	Incident management
9	Information Classification Policy	Cyber and information security
10	Information Security Awareness Policy	Training and awareness
11	Information Security Incident Management Policy	Incident management
12	IT Acceptable Usage Policy	Cyber and information security
13	Network Security Policy	Cyber and information security
14	Password Policy	Cyber and information security
15	Physical Security Policy	Cyber and information security
16	Privacy Notices	Privacy and information rights
17	Publication Scheme	Freedom of Information
18	Records Management Policy	Records and information

		management
19	Records Retention and Disposal Policy	Records and information management
20	Staff guidance on Data Protection and Freedom of Information Act (FOIA)	Guidance and awareness
21	Supply Chain Risk Management Policy	Cyber and information security
22	System Security Policy	Cyber and information security
23	Threat and Vulnerability Management Policy	Cyber and information security
24	User Endpoint Security Policy	Cyber and information security