INFORMATION GOVERNANCE FRAMEWORK

Organisation	Leeds Beckett University
Author(s)	Head of Information Governance
Developed in consultation with	University Registrar and Secretary Deputy Secretary Records and Information Governance Manager Information Compliance and Data Protection Manager
Owner	University Registrar and Secretary's Office
Target audience	Staff
Sensitivity	Public
Approved by	SIRO on behalf of UET – 21 December 2022
Endorsed by	
Effective date	December 2022
Review Date	+2 years from last date of approval [12-2024]
Status	
External references	
Links to other internal policies / procedures	Data Protection Policy Access to Information Policy Records Management Policy Information Asset Management Programme Information Asset Management Programme handbook Records Retention Schedule Information Classification Scheme Information Management and Security Policy Data Incident / Breach Procedure
Version reference	1.1
Version history and summary of changes	Previous version was dated June 2020. Changes made to reflect changes in legislation relating to international transfers, recognition of information sharing requirements and a new governance structure within the university.

INTRODUCTION

Information as a strategic asset

1. Information is a vital asset for all aspects of the University's operation and for the efficient management of the University'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 the University 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 the University and its future planning.

2. Information governance is concerned with how information is held, obtained, recorded, used and shared by an organisation. Information is used here as a collective term to cover terms such as data, documents, records and content. It is essential that the University has a robust information governance management framework, to ensure that information is effectively managed using the appropriate resources and documented policies, processes and procedures, staff training and the necessary management and accountability structures.

Purpose

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

Audience

4. This Framework applies to all staff the University and its partner organisations that, by agreement, have responsibility for any aspects of University information collection, maintenance or disposal.

Scope

5. The Framework relates to institutional or management data across but not limited to the following domains:
    *   Student data
    *   Staff data
    *   Research data
    *   Learning resource data
    *   Enterprise and community engagement data
    *   Business data
    *   Finance data
    *   Space and asset data

Definitions

6. Data are facts and statistics collected together for reference or analysis. When data is 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 the University's Information Governance Framework, the terms data and information can be used interchangeably.

THE INFORMATION GOVERNANCE FRAMEWORK

7. The Information Governance Framework sets out how Leeds Beckett University manages the capture, creation, access, security, management and sharing of its information both internally and externally.

8. The Framework has been developed based on best practice models adopted nationally and incorporates the expectations of the Information Commissioners Office as defined in their published self-assessment tool. It is structured around the following six key strands of activity:

   • Oversight and management of the Information Governance Framework
   • Records and Information Management
   • Information Compliance
   • Information Security and Cyber Security
   • Data Quality & Assurance
   • Information Sharing

9. A summary of each strand and what will be delivered through the adoption of this Framework is provided, alongside the supporting policies and procedures that will enable the framework to be implemented across the University.

10. The Framework will be underpinned by a supporting action plan and metrics to measure progress and success.

Information Governance - Roles and Responsibilities

11. The table below sets out the key roles and responsibilities relating to information governance throughout the management structures of the University. An overview diagram is attached at Appendix 1 and reporting structures Appendix 2.

Role	Responsibilities	Role Holder
University Executive Team (UET)	Key role in fostering the information governance culture within the university and the use of information and data as a strategic asset. In addition: • Providing Data Protection compliance assurance to the Board of Governors. • Receiving assurance and reports in relation to organisational compliance. • Enabling the DPO to perform their statutory requirements and is provided with the necessary time, resources and support. • Ensuring the DPO is involved as required in all issues which relate to the protection of personal data.	UET members UET through the Senior Information Risk Owner – Registrar and University Secretary
Senior Information Risk Owner (SIRO)	Senior management with overall responsibility for the use of information as a strategic asset in the university: • An Executive Director or Senior Management Board member who will implement and lead the organisation's Information Governance (IG) risk assessment and management processes within the organisation and advise the Board on the effectiveness of information risk management across the organisation. • Providing accountability and assurance to UET that information governance framework policies, including data protection, access to information and information security policies are complied with across areas. • Overview of any data protection breaches and responses. • Enabling the DPO to perform their statutory requirements and is provided with the necessary information and support. • Ensuring the DPO is involved as required in all issues which relate to the protection of personal data. • Receive any training as necessary.	University Registrar and Secretary

Role	Responsibilities	Role Holder
School / Service Information Risk Owners (SIROs)	Senior management with overall responsibility for the use of information as a strategic asset in their School or Service area line with university guidance: • Providing accountability and assurance to UET and the SIRO that information governance framework policies, including data protection, access to information and information security policies are complied with in their areas. • Management of responses to any data protection breaches in conjunction with the Information Compliance Team. • Enabling the DPO to perform their statutory requirements and is provided with the necessary information and support. • Ensuring the information compliance team is involved as required in all issues which relate to the protection of personal data. • Overview of information risks within the schools and services including risks arising from Data Protection Impact Assessments and Information Asset Registers. • Managing risks within their areas to feed into the corporate (using the risk management framework and appropriate steering group).	Deans & Directors
Data Protection Officer	A statutory role which advises on the University's compliance with data protection legislation: • Providing advice and recommendations to the SIROs and UET in relation to data protection risks. • Enabling and monitoring compliance with data protection legislation. • Reviewing and periodically reporting on the University's data protection compliance. • Advising the SIROs in relation to the management and response to any personal data breaches.Being the University's contact with the Information Commissioner's Office. The DPO role is independent and advisory and does not make decisions on the processing of personal data.	Head of Information Governance

Role	Responsibilities	Role Holder
Information Asset Owner	Role ensures that information assets are managed appropriately: • Ensuring consistent local information and data management processes are developed, implemented and reviewed. • Monitoring and reporting on information management and compliance as required to UET through Deans & Directors. • Role is responsible for data protection privacy compliance in their area and be the point of contact for the Information Compliance Team • Managing data protection risks. • Approval of DPIAs and Information Asset Registers (in conjunction with Deans and Directors so information risks can be captured on service / school information risk registers) • Maintenance of Information Asset Registers	School and Service Heads and Managers nominated by Deans & Directors
Information Asset Stewards/ Administrators	Information Asset Stewards/Administrators ensure that the daily operation and the quality of the data within systems and processes are compliant with the Information Governance Framework and related policies and procedures. They take a proactive role in understanding the purpose of the processes they operate and how they contribute to the wider University and undertake required learning and development activities.	Individuals nominated by IAOs
All staff and third parties	All individuals and organisations who process information on behalf of the University 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.	

OVERSIGHT AND MANAGEMENT OF INFORMATON GOVERNANCE

11. This strand of the Framework covers the management of information governance at an institutional, managerial and operational level across the University. It is a fundamental component of the Framework as it will provide the necessary ownership, advocacy and accountability structures that can be used to ensure the appropriate prioritisation and implementation of the information governance framework across the University.

12. The following measures will be implemented to ensure appropriate oversight and management of the University's approach to Information Governance:

REF	Measures
IG 1	There are clearly defined corporate, managerial and operational responsibilities for information governance appropriately embedded in role expectations across the University.
IG 2	Leeds Beckett University has a Strategic Data Management Group with oversight for Information Governance supported by an Information Management Operations Group with agreed Terms of Reference. These Groups will work within and report to an appropriate place within the University's broader executive advisory group and corporate governance arrangements. (Appendix 2)
IG 3	The Strategic Data Management Group and its Information Management Operations Group have access to the necessary expertise across all areas of the Framework.
IG 4	A corporate information governance improvement plan sets out priorities and objectives and is managed by the Information Management Operations Group and monitored by the Strategic Data Management Group.
IG 5	Leeds Beckett University has an Information Asset Management Training Programme that includes Data Protection and Privacy by Design requirements.
IG 6	An established annual review process exists to maintain the currency of the Information Governance Framework within the University.
IG 7	There are clearly defined Information Governance Policies which are reviewed on a 3 yearly basis to reflect changes to external influencing factors and changes in legislation.

13. The following policies and procedures will support the delivery of the Information Governance Management measures outlined above.

- Suite of Information Governance Policies
- Leeds Beckett University Information Governance Framework
- Strategic Data Management Steering Group Terms of Reference
- Information Management Operations Group Terms of Reference
- Corporate Information Governance Improvement Plan
- Leeds Beckett University Information Asset Management Training Programme
- Information Governance & Security – Staff guidance materials

RECORDS AND INFORMATION MANAGEMENT

14. Records and Information Management covers the process of creating, describing, using, storing, archiving and disposing of organisational records. This framework considers alignment to the International Standard or Records Management, ISO 15489, which provides the guiding principles around which the University's records and information management is designed and built. It is a fundamental component of the Information Governance Framework as it ensures the University's records sets enable adherence to compliance rules and statutory access requirements as well as protecting the University's corporate memory.

15. The following measures will ensure the delivery of an appropriate Records Management function:

REF	Measure
RM 1	Leeds Beckett University has Records Management Policy.
RM 2	Leeds Beckett University has an agreed and implemented Records Retention Schedule.
RM 3	Leeds Beckett University has agreed and implemented Information Management and Security Policy that include security & access measures and controls.
RM 4	Leeds Beckett University has documented procedures to ensure delivery of the Records Management Policy. As a minimum, these should cover: • Storage and Handling • Business Continuity • Access, Retrieval and Disposal
RM 5	Leeds Beckett University has deployed appropriate systems and tools to efficiently manage the University's records in line with the Records Management Policy.
RM 6	A Controlled Business Vocabulary (or taxonomy) is developed and embedded within electronic document and records management processes.
RM 7	Leeds Beckett University has a Records Manager that has the required capacity and skills to develop and support Information Asset Owners in the implementation and embedding of the Records Management Policy.
RM 8	Core Records Management competencies are built into appropriate role expectations and a suitable training and development programme established to facilitate their delivery.
RM 9	Leeds Beckett University has agreed and implemented an Information Classification Scheme which incorporates security rules and builds privacy and retention by design into recordkeeping architecture.
RM 10	Leeds Beckett University has robust Information Asset Registers in place across the institution which details information processing specifics including the lawful basis, storage and sharing arrangements.

16. The following policies and procedures will support the delivery of the Records Management measures outlined above.

- Records Management Policy
- Records Retention Schedule
- Guidance on Records Management
- Information Classification Scheme

INFORMATION COMPLIANCE

17. Information Compliance covers the legal framework and the standards that need to be established to ensure the University's management of information operates within the law and the rights of individuals.

18. The University manages and processes large volumes of confidential and sensitive information about people. It must deal with this lawfully and ethically. Failure to do so could cause harm and distress to individuals and cause reputational damage and increased risk of litigation or regulatory action. The key legislation the University must comply with includes the UK General Data Protection Regulation, UK Data Protection Act, the Freedom of Information Act and the Human Rights Act.

19. The following measures will support the delivery of an appropriate Information Rights and Compliance function:

REF	Measures
IC 1	Leeds Beckett University has an up to date, approved and monitored Access to Information Policy that sets out University procedures, roles and responsibilities and incorporates access to information through information sharing.
IC 2	Schools and Services have nominated staff responsible for supporting Access to Information requests.
IC 3	Leeds Beckett University has a corporate framework for evaluating the public interest test for disclosing information through Access to Information requests in a consistent and transparent manner.
IC 4	All staff and the public are aware of the various rights of access to information under Data Protection/GDPR and Freedom of Information and how these can be exercised inclusively.
IC 5	Information requests are provided in the most appropriately accessible format within statutory timescales.
IC 6	Leeds Beckett University has an effective mechanism in place to consider appeals to withhold information under information law.
IC 7	Leeds Beckett University has an up to date, approved and monitored Data Protection Policy compliant with data protection principles and statutory requirements.
IC 8	Leeds Beckett University has an effective process for the reporting, management and monitoring of all incidents / breaches in line with the requirements of the ICO.
IC 9	The requirement to complete Data Protection Impact Assessments is clearly defined across the University and effective mechanisms are in place to identify, record, manage and mitigate emerging risks.

IC 10	Leeds Beckett University provide accessible information to individuals about the use of their personal information (data) through the publication of privacy notices and statements which contain all the information required under Articles 13 and 14 of the UK GDPR.
IC 11	Staff are aware of the Data Protection Act and Information Governance policies and procedures relevant to their role, appropriate training is provided and relevant material is made readily accessible.
IC 12	Leeds Beckett University has appropriate procedures, measures and continuity plans to identify, record and manage information risks.

20. The following policies and procedures support the delivery of the information compliance measures outlined above.

- Data Protection Policy
- Access to Information Policy
- Publication Scheme
- Staff guidance on Data Protection and Freedom of Information Act (FOIA)
- Guidance on Data Protection Impact Assessments
- Information Asset Management Programme
- Information Governance Training Needs Assessment and Training Plan
- Privacy Notices
- Incident/Breach reporting procedure and guidance

DATA QUALITY AND ASSURANCE

21. This strand of the Framework covers the need to ensure the quality, accuracy, and reliability of our data and internal information. It is a fundamental component of the Information Governance Framework as, staff, students and key stakeholders need to be able to trust the validity and authority of corporate information sources and have confidence that it is up-to-date and accurate.

22. It is important that the University can assess the quality of its data as a strategic asset and business intelligence tool and ensures that all data returns comply with the necessary statutory and regulatory requirements and standards.

23. The following measures will support the delivery and assurance of data quality across the various areas of the University with responsibility for data quality and data returns:

REF	Measures
DQ 1	Leeds Beckett University has a commitment to data quality and has a designated data lead at executive level.
DQ 2	Leeds Beckett University has a Data Quality Management Policy implemented across Schools and Services with the scope to ensure data quality of all information. This is supported by documented data quality processes and procedures specific to business activity and systems.
DQ 3	There are designated data stewardship roles with specific responsibility for data quality across the University embedded into the roles of Information Asset Owners and Information Asset Administrators.
DQ 4	Standards are set through processes and procedures to ensure quality data is being submitted as part of external returns and shared with external organisations.
DQ 5	There are documented procedures and processes in place governing the capturing, recording and handling of data.
DQ 6	There are arrangements in place to oversee / review the appropriateness of any documented procedures for data collection and determining accuracy.
DQ 7	Data quality checks are incorporated into processes and procedures around the handling of personal data.

24. The following policies and procedures support the delivery of the data quality assurance measures outlined above:

   •   Data Quality Management Policy
   •   Data Quality and Auditing Procedures
   •   Records Retention Schedule

INFORMATION SECURITY AND CYBER SECURITY

25.   Information security covers the policies and procedures in place to protect information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction.   It is one of the fundamental components of the Information Governance Framework as it will ensure the University is able to protect the confidentiality, integrity and availability of information within the organisation, that includes cyber security resilience.

26.   The following measures will support the delivery of an effective and robust Information Security function:

REF	Measures
IS 1	There is an Information Management and Security Policy in place based on ISO 270001
IS 2	Roles and responsibilities for adherence to the policy are clearly defined and an appropriate training programme is in place for relevant roles.
IS 3	There is an inventory of system assets as required for compliance with data protection principles which are used to assess information and protection risks.
IS 4	Physical and IT access controls are in line with the security policy and the need for information dissemination and authorisation
IS 5	A Corporate Risk Management & Assurance Framework is in place and information security risks are incorporated. Cyber security form part of the corporate risks
IS 6	Security requirements are included in formal system acquisition, development and maintenance procedures along with Data Protection Impact Assessments where required.
IS 7	There are procedures to report information security incidents and weaknesses and to escalate action on dealing with these. Staff are made fully aware of the procedures and these are embedded within the organisation
IS 8	There is a business continuity management process designed to limit the impact of and recover from the loss of information assets.
IS 9	All changes to information processes are planned and implementation and is effectively managed including the use of Data Protection Impact Assessments.
IS 10	The IT systems and environment are managed and controlled to protect them from information and cyber security threats using risk based approaches.
IS 11	Contract management – appropriate security arrangements are in place for incorporated cyber essentials / accreditations contract expectations
IS12	There is clear alignment between our IT security, information governance and HR disciplinary policies to ensure adherence and compliance.

27.   The following policies and procedures support the delivery of the University's Information Security measures outlined above:

- Information Management and Security Policy
- IT Security Policy
- IT for New Starters Manual
- Bring Your Own Device Policy
- Computer Protection Policy
- Cryptography Policy
- Information Handling Policy
- Network Management Policy
- Software Management Policy
- System Planning & Management Policy
- User Management Policy
- Use of Computers Policy
- Wireless Communication Policy
- Mobile Computing Policy
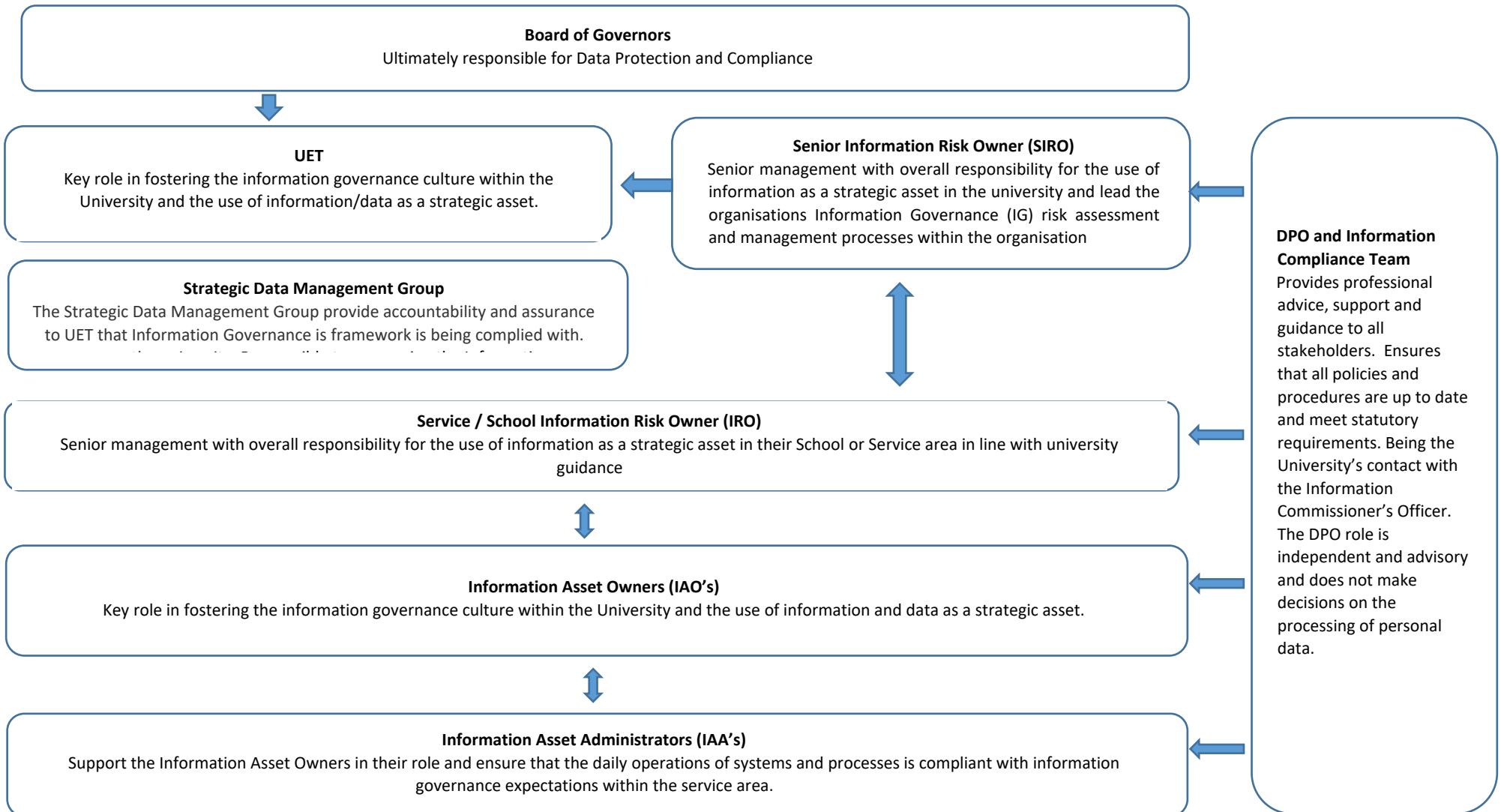- HR Disciplinary Policy

INFORMATION SHARING

28. Data Protection Law facilities data sharing when is approached in a fair and proportionate way. Data Protection Law is an enabler for fair and proportionate data sharing rather than a blocker. This strand of the framework covers the need to ensure that any personal data being shared is done so in compliance with Data Protection Law as outlined in the statutory code of practice made under section 121 of the Data Protection Act 2018.

29. The following measures will support the delivery and assurance of information sharing across the various areas of the University who need to share personal information with internal and external stakeholders:

REF	Measures
ISH 1	There is an Information Sharing Policy in place based on the statutory code of practice.
ISH 2	Leeds Beckett University ensures that sharing of personal information (including restricted transfers) is supported by the relevant agreements as clauses and clearly set out responsibilities in relation to data sharing.
ISH 3	Due diligence to guarantee contractors implement appropriate information sharing technical and organisational measures to meet Data Protection / GDPR requirements is conducted.

30. The following policies and procedures support the delivery of the University's Information Sharing measures outlined above:

   • Information Governance Procurement Due Diligence and procedures
   • Partnerships and contract sign off procedures including due diligence
   • Information Sharing Agreement Templates (Legal Services)

Appendix 1 - Roles and responsibilities for the management and governance of Information Assets within Leeds Beckett University

Board of Governors
Ultimately responsible for Data Protection and Compliance

UET
Key role in fostering the information governance culture within the University and the use of information/data as a strategic asset.

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 organisations Information Governance (IG) risk assessment and management processes within the organisation

DPO and Information Compliance Team
Provides professional advice, support and guidance to all stakeholders. Ensures that all policies and procedures are up to date and meet statutory requirements. Being the University's contact with the Information Commissioner's Officer. The DPO role is independent and advisory and does not make decisions on the processing of personal data.

Strategic Data Management Group
The Strategic Data Management Group provide accountability and assurance to UET that Information Governance is framework is being complied with.

Service / School Information Risk Owner (IRO)
Senior management with overall responsibility for the use of information as a strategic asset in their School or Service area in line with university guidance

Information Asset Owners (IAO's)
Key role in fostering the information governance culture within the University and the use of information and data as a strategic asset.

Information Asset Administrators (IAA's)
Support the Information Asset Owners in their role and ensure that the daily operations of systems and processes is compliant with information governance expectations within the service area.

Information Asset - identified electronic or paper filing/storage systems that holds a named common set of records, e.g. employee record, finance and business information, complaint files etc.

Appendix 2 - Information Governance Framework – Oversight & Operations Groups

Group	Description	Membership
Strategic Data Management Group (SDMG)	Responsible for overseeing a University wide Information Governance Framework that supports effective information management - planning, developing and maintaining policies, standards, procedures and guidance, coordinating information governance activity across the University.	Director of Strategic Insight and Business Analysis (Chair), SIROs, IAOs of systems that process personal information
Information Management Operations Group (IMOG)	Operational arm of SDMG, tasked with the development and implementation of policies and processes. Provides professional guidance on best practice regarding the lifecycle for the creation, collection, curation, security and governance, access or usage, disposal or retention and preservation, of any records, information and data assets required and managed by the University. this group brings together data, records, information and security specialists from across the University	Head of Information Governance, IT Security Manager, Records Manager, Schools and Service representative responsible for key aspects of University data, records and information
Task and Finish Groups	Groups of Information Asset Stewards / Administrators established, as required, to work collaboratively on specific data and information processes to apply University and regulatory requirements, standards of best practice and adapt them for local implementation in their operational areas.	As nominated by Deans and Directors