UNIVERSITY of HULL

Information Governance and Assurance Policy

Classification	Policy
Version number:	4-00
Status	Approved
Approved by:	Information Governance Committee
Approval date:	22 October 2024
Effective from:	23 October 2024
Next review date:	22 October 2026
Document author:	University Secretary, Registrar and Chief Compliance Officer
Document owner:	University Secretary, Registrar and Chief Compliance Officer
Contact:	University Secretary Office

Collaborative provision: Not mandatory
State whether this document is applicable to the University's collaborative partners

Related documents: Data Protection Policy; Data Breach Policy; Data Protection Privacy Impact Assessment Policy; Records Management Policy; Data Retention Schedule; Data Classification and Handling Policy; Information Governance & Assurance Framework; Information Security Controls Policy; Information Systems Security and Architecture Policy

University document: Yes
A University document applies across the institution, is approved by a committee of Council or Senate and is held in the University Policy Directory on SharePoint.

Published location: University Policy Directory SharePoint

- The University has adopted the principles of Designing for Diverse Learners, and all policy documents should be written with reference to these principles. Further information is available at the **Designing for diverse learners website**.
- An Equality Impact Assessment (EIA) must be considered for all new and amended policies. Further information is available from the **EIA section of SharePoint**.
- This document is available in alternative formats from **policy@hull.ac.uk**.
- All printed or downloaded versions of this document are classified as uncontrolled

Information Governance and Assurance Policy

Table of Contents

Information Governance and Assurance Policy

1 Introduction

1.1 Information Assurance is the name given to the governance framework by which an organisation both protects, and ensures its ability to use, the information it owns. It is a risk-based process for managing the use, processing, storage, and transmission of information and the systems and processes used for those purposes.

1.2 Information is essential to the governance, management, administration and operation of the University. Therefore, the security and effective control of the University's information is fundamental to its success. Failure to manage information security and compliance can result in serious financial, commercial or reputational damage and/or legal proceedings.

1.3 This overarching policy includes a set of sub-policies and other documents which, taken together, constitute the Information Governance and Assurance Framework for the University.

2 Purpose

2.1 This policy establishes the University's commitment to Information Assurance through effective governance. The policy's aim is to set out how the University seeks to assure its information assets through a risk-based, proportionate framework of governance controls.

2.2 This framework establishes that the University will:

a. ensure confidentiality of information, by protecting assets against unauthorised disclosure;

b. preserve information integrity, by protecting assets from unauthorised or accidental modification;

c. maintain availability of information, by ensuring that assets are accessible as and when required by those authorised to do so; and

d. ensure compliance with all legal and statutory requirements.

2.3 The framework ensures that policy implementations are measurable, thus enabling the University to demonstrate and report on the overall progress and maturity of its Information Assurance and Governance programme.

3 Scope

3.1 This policy and its sub-policies apply to all information assets for which the University is responsible.

3.2 The National Archives[1] defines an Information Asset as 'a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently'. As such, an information asset might be a database, information system or a set of paper files relating to a specific large project.

3.3 This policy and its sub-policies apply to all members of the University and any others

[1] Information Asset factsheet (2017): http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

who may process information on its behalf.

4 Roles and responsibilities

4.1 The Information Governance Committee (IGC) will be responsible for approving the Information Governance and Assurance Policy and the subsidiary policies included within the overarching policy framework. Approvals of significant amendments to the Information Governance and Assurance Policy Framework will be reported to the University Leadership Team (ULT) for information.

4.2 The University Secretary, Registrar and Chief Compliance Officer is the University Senior Information Risk Owner (SIRO) and takes responsibility for operating a framework for assessing risks to information across the organisation and is responsible for approving unusual or controversial information governance and assurance decisions.

4.3 Executive Senior Information Risk Owners (Executive SIROs), as members of ULT, will be accountable for information assets within their remit. Executive SIROs will appoint System Owners to safeguard assets on their behalf.

4.4 System Owners are expected to understand at a high-level the purpose of the information assets for which they are responsible, including how information is stored, processed, transferred and/or shared. They will also be responsible for ensuring that adequate resource is directed to managing information assurance activities in accordance with this policy. System Owners will provide reports and escalate risks to their Executive SIRO as necessary. System Owners will appoint System Stewards to manage assurance activities on a day-to-day basis.

4.5 System Stewards are expected to understand in great depth the purpose of an information asset, and possess detailed knowledge of how information is stored, processed, transferred and/or shared. They will work with Data Protection, Legal, and Information Security specialists to ensure the objectives of this policy are effectively met, and that the controls within the overarching governance framework are applied, reporting any risks to the System Owner as necessary.

4.6 Data Owners accountable for the fitness for purpose of defined data area or domains, including Student, Finance, Estates and staff data. Data owners are responsible for ensuring the data within their domain (no matter where stored) is fit for both operational and strategic use on behalf of the University.

4.7 Data Stewards responsible for the definition and quality of defined dataset(s). The focus of this role is defining the meaning of data and determining the relevant data quality checks and controls required to maintain defined levels of data quality, in line with University's operational and strategic.

4.8 The information asset will assist to determine the role requirement and in some cases the role may overlap e.g. System Owner will also be Data Owner.

4.9 Governance and Compliance and ICT Services will be responsible for providing guidance and support to IGC, Executive SIROs, System Owners and System Stewards in order that they may fulfil their obligations under this policy and within the wider framework.

4.10 Governance and Compliance and ICT Service will be responsible for the development, operation and maintenance of the Information Security Management System (ISMS) that forms part of the wider framework. They will also report on overall compliance to IGC.

5 Principles and implementation

5.1 The University will safeguard its information assets through the application of appropriate organisational and technical measures.

5.2 The University will maintain a risk management regime to support the oversight and management of information risks.

5.3 The University will maintain a register(s) of Information Systems/Services to determine and maintain the existence, ownership and accountability of information assets and to support the management of information assurance activities.

5.4 Custodian roles will be assigned for all information assets as described in Section 4.

5.5 All information assets will be classified in accordance with the Data Classification and Handling Policy.

5.6 The privacy impact of all information assets must be considered in line with the provisions of the Data Protection Impact Assessment Policy.

5.7 Where a data processor is involved in the creation, acquisition, processing or maintenance of information assets, the principles within this policy will apply equally to the data processor. This will usually be ensured via a Data Processing Agreement in accordance with the Data Protection Policy.

5.8 The intended lifecycle of an asset, including implementation, operating lifetime, and decommissioning should be clearly outlined and documented.

5.9 The availability requirements for information assets should be clearly defined and documented (for example, via a Business Impact Analysis and Business Continuity Plan), and should be based on the University's strategic, operational or regulatory needs.

5.10 The University will design and implement an Information Security Management System (ISMS) in line with the provisions of internationally recognised standards or frameworks, such as ISO/IEC 27001. All information assets will be subject to the requirements of the ISMS to ensure that this policy has sufficient coverage.

5.11 Sufficient resources must be allocated to the ongoing support and maintenance of information assets. Managerial, operational and technical requirements should be considered individually.

5.12 More stringent, additional policies and codes of practice may be required for specific areas of the University, e.g. where staff working with identifiable health data must comply with the requirements of the NHS Data Security and Protection Toolkit. Such additional policies and codes of practice may be locally approved and applied within specific areas, but will augment rather than replace policies, guidelines and codes of practice in operation across the University.

6 Compliance

6.1 Those responsible shall ensure that all relevant information assurance controls within the wider governance framework are implemented correctly within their area of responsibility to achieve compliance with this policy.

6.2 Compliance with this policy and its subsidiary policies will be supported by:

a. evidentiary reviews, including quality assurance and testing activities; and

b. monitoring, auditing and reporting of network and information system activity.

6.3 Any breaches of policy, or deliberate non-compliance with policy will be investigated, reported and may be treated as misconduct under the appropriate staff or student disciplinary policy. Failure to carry out mandatory actions within this and related policies may be considered a breach of the relevant policy.

6.4 In the event that an employee or student is aware of a potential breach of this policy, they are encouraged to report their concerns to their manager or Head of Department.

7 Version control

Version	Author	Date approved	Relevant sections
4-00	University Secretary, Registrar and Chief Compliance Officer	22/10/2024	-