UNIVERSITY OF HULL

Information Governance and Assurance Policy

Document Classification:	Policy
Version Number:	3.0
Status:	Approved
Approved by (Board):	Information Governance Committee (IGC)
Approval Date:	11 October 2021
Effective from:	11 October 2021
Next Review Date:	Biennual
Document Authors:	Stewart Doyle
Document Owner:	Chief Compliance Officer, Governance and Compliance (Chris Ince)
Department/Contact:	infocompliance@hull.ac.uk
Summary:	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.
Scope:	This policy applies to all University members
Collaborative provision:	
Assessment: (where relevant)	
Consultation: (where relevant)	
Relevant legal frameworks:	See section 8, 'Relevant legislation' below
Related documents:	See section 7, 'Subsidiary Policy list' below
Published locations:	University website (www.hull.ac.uk/policies)
Document Communication and Implementation Plan:	Available upon request.

1. Introduction

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.

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.

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

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.

This framework establishes that the University will:

- Ensure **confidentiality** of information, by protecting assets against unauthorised disclosure;
- Preserve information **integrity**, by protecting assets from unauthorised or accidental modification;
- Maintain **availability** of information, by ensuring that assets are accessible as and when required by those authorised to do so; and,
- Ensure **compliance** with all legal and statutory requirements.

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

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

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.

This policy and its sub-policies apply to all members of the University and any others who may process information on its behalf.

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

4. Roles and Responsibilities

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.

The 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.

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

Information 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. Information System Owners will provide reports and escalate risks to their Executive SIRO as necessary. Information System Owners will appoint Information System Stewards to manage assurance activities on a day-to-day basis.

Information 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 Information System Owner as necessary.

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

Governance and Compliance and ICT 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

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

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

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.

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

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

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

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.

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

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.

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.

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

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 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

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.

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

- Evidentiary reviews, including quality assurance and testing activities; and,
- Monitoring, auditing and reporting of network and information system activity;

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.

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. Subsidiary Policy list

Subsidiary policies shall be considered part of this policy and shall have equal standing. The following list of current and proposed subsidiary policies may be added to via the governance arrangements described above:

- Data Protection Policy
- Breach Management Policy
- Data Protection Impact Assessment Policy
- Data Retention Policy
- Retention Schedule
- Data Classification and Handling Policy
- CCTV Policy
- Photography Policy
- Data Sharing Policy
- Information Security Controls Policy
- Information Systems Security and Architecture Policy

8. Relevant legislation

The University will comply with all legislation and statutory requirements relevant to information and information systems, including, but not limited to:

- Computer Misuse Act 1990;
- Data Protection Act 2018 and the General Data Protection Regulation (GDPR);
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006; and,
- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018