Information Asset Management Policy

Document Control

Responsibility for Policy:	Chief Information Officer
Approved by and date:	UEB 19th March 2024
Frequency of Review:	Annual
Next Review date:	February 2025
Related Policies:	Information Security Policy GDPR Data Breach Procedure
Minor Revisions:	

1. Glossary of Terms

DAR - Data Asset Register

IAO - Information Asset Owner

IAR – Information Asset Register

SIRO - Senior Information Risk Owner

2. Background

An information asset is a body of information that facilitates the business carried out by the University and that, thereafter, is retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy, electronically or held on film, microfiche or other media.

The University holds a large amount of information in different formats and in a variety of locations and systems. The efficient management of the records is necessary to support the core functions, to comply with legal and regulatory obligations and to contribute to the effective running of the institution.

Managing this information requires the University to have Information Asset Registers (IAR) that are controlled by Information Asset Owners. The IAR is a mechanism for understanding and managing assets and the risks to them. It includes links between the assets, their business requirements or processes and any technical dependencies that there may be. It is dynamic and should be constantly updated and enhanced to ensure each area develops a solid understanding of the information that it holds.

3. Scope of the policy

2.1 This policy applies to all information created, received or maintained by the University in the course of carrying out teaching, assessment, scholarly, administrative or management functions.

2.2 This policy applies to all students, staff and visitors to the University along with those contracted to work at or for the University. Staff include consultants, contractors, volunteers, casual workers and agency workers. Those applying to work or study at the University are also included.

2.3 The policy applies to all University owned / licensed data and software whether loaded on university or privately / externally owned systems when connected to the University network directly or indirectly, and to all data and software provided to the University by sponsors or external agencies.

4. Requirements of the Policy

All users must abide by the following regulations: -

Compliance with all University policies including, but not restricted to:

- IT Acceptable Use Policy
- Information Security Policy
- Data Protection Policy
- Portable Data Device Security Policy
- E-mail Policy

Compliance with all applicable laws and regulations including but not restricted to:

- Computer Misuse Act (1990) which makes activities such as hacking or the deliberate introduction of viruses a criminal offence
- Criminal Justice Act 1994 amendment to the Obscene Publications Act under which it is a criminal offence to create, store, download or transmit obscene material
- Data Protection Act 2018
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Freedom of Information Act 2000
- Copyright Designs and Patents Act 1988
- Malicious Communication Act 1998
- Counter-Terrorism and Security Act 2015

In addition, the storage, processing and transmission of payment card information must be conducted in accordance with Payment Card Industry Data Security Standards (PCI DSS) mandatory requirements.

5. Data Asset Register (DAR)

The Data Asset Register sets out:

- The University electronic assets
- The owner of each asset
- The business and system process the asset is used for
- Where the information is held and how it is updated
- Whether it contains personal data
- Whether a retention schedule exists
- Key users of the information

The DAR is dynamic and should be constantly updated and improved to ensure that there is a full understanding of the information held.

The latest DAR can be accessed via the University Documents section of MyReports.

6. Roles and Responsibilities

All users who access University information must play their part in safeguarding the availability, integrity, confidentiality and authenticity of the information they hold or access.
Alongside this, there are a number of specific roles that will be executed by designated staff. These are:

Senior Information Risk Owner (SIRO)

The members of the University Executive Board will undertake this role taking ownership of the University's information risk, act as an advocate for information risk and provide advice on the information risk governance and risk exposure. The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its clients and stakeholders

- Owning the University's overall information risk policy and risk assessment processes and ensuring they are implemented consistently
- Advising the Vice Chancellor and relevant accounting officers on the information risk aspects of internal controls

Information Asset Owner (IAO)

This role will be executed by senior members of staff responsible for the protection of designated Information Assets. They may delegate information security tasks to managers or other individuals but remain accountable for the proper implementation of the tasks.

The IAO is expected to understand the overall business goals of the University and how the information assets they have responsibility for contribute to and affect these goals.

The risks to be managed by the IAO are:

- Assuring against inappropriate access to, or disclosure of, protectively marked or sensitive personal information by staff, students, contractors and outsiders, whether accidental or deliberate
- Inappropriate sharing of information
- Internal threats for example staff acting in error or deliberately, or external parties obtaining information illegally and exposing it / acting maliciously to defraud
- Information loss – particularly during transfer or movement of information, or as a result of business or regulatory change
- Loss of ready access to information
- Ensuring that Information assets are not retained for longer than required (either by law or for business need)

The responsibilities are:

- Leading and fostering a culture that values, protects and uses information for the University good
- Knowing what information is held within the asset, what information is transferred in or out of it and what systems it links to
- Knowing who has access and why, ensuring that their use is monitored and arranging for access to be removed when no longer required.
- Understanding and addressing risks to the asset and ensuring that any information loss incidents are reported and managed within the University's GDPR Data Breach Procedure.

- Ensuring compliance with all relevant University policies and all regulatory requirements as they relate to the information assets
- Ensuring the appropriate classification and protection of the information assets
- Ensuring that all staff utilising information assets are appropriately trained in managing, securing and accessing the assets
- Determining appropriate criteria for granting access to information assets
- Authorising access to information assets in accordance with the business need
- Ensuring that contractual agreements exist for the transfer to, or processing by, any third party
- Defining the appropriate information retention schedules for each asset and ensuring that information is deleted in line with those schedules

Information Leads

This role will be executed by staff identified by the Information Asset Owners.

Information Leads will be expected to:

- Review the DAR on a six-monthly basis and ensure that it is maintained and updated when new assets are created
- Ensure that retention periods for information are defined in the Retention Schedule document
- Arrange for documented audits to ensure that information is deleted in accordance with retention periods
- Ensure that decisions are clearly recorded against any information that is retained over its agreed retention period
- Ensure that designated staff understand the importance of maintaining correct access controls to information
- Carry out regular audits to ensure that correct access controls are maintained
- Provide assurance to IAO on a regular basis
- Attend training as required

7. Annual Report

IAOs will be required to provide annual assurance on the following areas to the SIRO:

- that local procedures governing the use of information are in place and updated when required

- that access control measures are in place for information that includes how access is granted and removed for users
- that action following security incidents are monitored and updated
- that any records management responsibilities are captured e.g. retention schedules are reviewed annually and systems used to store information have been reviewed to ensure retention is reflected
- contracts with third parties have the agreed information security and GDPR clauses and compliance with these are monitored
- that actions identified during audits are captured in the DAR where required

8. Storage

All records should be stored with due regard for appropriateness, efficiency, cost effectiveness and security. It is the intention of the University to digitise information where possible and when resources allow.

Confidential and sensitive records should be stored securely, in locked cabinets if held in hard copy and in line with the Information Security Policy if held electronically.

9. Disposal of Information

Personal, confidential and business critical information must be disposed of in a secure manner.

For paper information, items should either be

- cross-shredded onsite or
- placed in the Confidential Information Consoles positioned around the campuses.

For electronic information: -

- DVDs / CDs should be shredded and then put into a recycling unit
- Computer hard drives and external storage media (USB, detachable hard drives etc) should be wiped with a suitable software tool. No unencrypted data should remain on these types of media before re-using / recycling / disposal
- Media that cannot be wiped initially will need to be protected before being overwritten e.g. kept in a locked safe

10. Policy Awareness and Disciplinary Procedures

This policy will be made available to all users via the governance section of the University website maintained by the Legal Services Governance & Risk Office. Staff, students, authorized third parties and contractors given access to University information will be advised of the existence of the relevant policies, codes of conduct and guidelines.

Failure to comply with the policy may lead to suspension or withdrawal of an individual's access to information systems.

11. Policy Review

This policy will be reviewed on an annual basis to identify any required revision