Document/Report Title	**Information Strategy**
Status	Approved
Author	Craig Hutchinson-Howorth
Version	2.0
Date Approved	June 2018
Circulation	Information Governance Board / Information Strategy Group

Principles and Governance

The implementation of efficient information systems, the collation & analysis of transactional data and the use of effective business intelligence information supports the University in reaching its strategic aims. The Information Strategy aims to outline the overarching principles the University takes in prioritising and developing its information environment and technology infrastructure; and in managing the data assets contained therein.

Scope

The Information Strategy covers all staff who create, store, share and dispose of information. It sets out the overarching principles, policies and responsibilities relating to the management and sharing of information including those with stakeholders, partners and suppliers. The Strategy concerns the management of all paper and electronic information and its associated systems within the organisation, as well as information held outside the organisation that affects its regulatory and legal obligations.

Policies

The Information Strategy incorporates a number of specific policies. Individual policies are maintained by the University's Information Governance Office within the Strategic Planning and Policy Unit. Policies are agreed by the University's Information Strategy Group. A review of all policies is undertaken on an annual basis by the Information Governance Board.

Overarching Principles

The overarching principles are designed to provide a framework for the facilitation and delivery of the key aims they are:

i. *Information is a strategic asset.* The recognition of the strategic benefits of excellent information management is critical to achieving the University's ambitions; all corporate systems should enable the creation, capture, analysis, publication, storage and archiving of all data efficiently and with minimum duplication, acknowledging the varying levels of security which need to be applied.

ii. *Information leads to innovation*. Opportunities will exist to exploit and develop the intelligent use of data in support of new and enhanced learning activities; sharing good practice through information exchange, training and development and the nurturing of communities of practice both internal and external to the University to provide a fertile environment for discovery.

iii. *Information is key to the success of a learning organisation.* The University will need to remain competitive to operate in a market focussed environment. Information and data management systems should be designed to encourage the sharing of key data across the University whilst remaining cognisant of the requirements placed on an organisation by the General Data Protection Regulations. To achieve this, shared values and skills will be nurtured to develop effective internal communication processes. The development of an information governance culture which prioritises the following enabling characteristics is important to the successful delivery of the strategy.

a. *Information is owned*. The information environment should be managed to ensure that there is access to data which is; accurate, valid, reliable, timely, relevant and complete. University systems and processes must have an identified owner who provides assurance as to the effective and efficient management of information in their area, including the integration with core organisational systems. All staff have a responsibility to become stewards of the information they collect, store, process and analyse, they are responsible for ensuring the quality of the data is maintained, working to agreed information standards and access policies.

b. *Information is supported by a first-class IT infrastructure*. The development of a resilient, reliable and secure IT infrastructure is required to support a managed and integrated electronic information environment. The IT infrastructure should support regulated access to the secure storage and dissemination of information.

c. *Information should be available and accessible within the guidelines set out by the appropriate legislation.* Stakeholders should be able to access information flexibly according to need, and in compliance with the University's overarching policies. In particular the University has a duty to take additional care when managing personal confidential information and should ensure compliance with the relevant legislation.

The University aims to manage personal confidential information in line with the key principles outlined below.

i. *Justify the purpose.* Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined and documented, with continuing use regularly reviewed, by an appropriate officer.

ii. *Personal confidential data should only be used as necessary.* Personal confidential data items should not be used unless the data is required to satisfy a specified purpose, as outlined under the General Data Protection Regulations. The need for individual students to be identified should be considered at each stage of a process.

iii. *Use the minimum necessary personal confidential data.* Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or is accessible as is necessary for a given function to be carried out.

iv. *Access to personal confidential data should be on a need-to-know basis.* Access to personal data should be limited to those who can demonstrate a particular requirement, the data provided should be limited to that needed to fulfil the identified task. This may result in the use of access controls or in the splitting of data flows where one data flow is used for several purposes.

v. *Everyone with access to personal confidential data should be aware of their responsibilities*. Action should be taken to ensure that those handling personal confidential data; both academic and administrative staff, are made fully aware of their responsibilities and obligations to respect student confidentiality.

vi. *Comply with the law.* Every use of personal confidential data must be lawful. The University's Directorate has overall responsibility for ensuring that the organisation complies with legal requirements.

vii. *The duty to share information can be as important as the duty to protect student confidentiality.* Education professionals should have the confidence to share information in

the best interests of their students within the framework set out by these principles. They should be supported by the policies of the University, regulators and professional bodies.

Governance

The University's strategies are determined by the Directorate with referral on to the Governing Body, Academic Board and their subsidiary committees where appropriate. The responsibilities and reporting guidelines for each group are as below.

I. Directorate

i. Responsibilities
   a. To oversee and assure all aspects of the University's information governance systems including the overarching policies, procedures and systems.
   b. To provide guidance with respect questions requested under the Freedom of Information Act.
   c. To report any issues or concerns arising from the organisational information governance systems to the University Governing and Regulatory bodies as appropriate.

ii. Reporting
   a. Annual reports regarding data quality are submitted as part of the regulatory annual accountability process.
   b. Issues are reported to the University's Audit Committee on a by incident basis, including the reporting of any regulatory breaches under consideration by the Information Commissioner's Office.

II. Information Strategy Group

i. Responsibilities
   a. To provide institutional leadership for and ownership of the Information Strategy and related infrastructure, services and support developments.
   b. To support the development, monitoring and evaluation of the institutional Information Strategy.
   c. To advise Directorate on the further development of institutional resources to support the Information Strategy.
   d. To monitor and make recommendations for the provision and enhancement of learning support, user support and staff development in relation to the Information Strategy.
   e. To provide a forum and mechanism for the sharing and dissemination of good practice in this area.
   f. To monitor regional and national developments in this area with a view to timely and appropriate institutional participation.
   g. To coordinate the review and development of current and future information systems in line with the agreed Information Strategy and agreed University priorities.
   h. To ensure the clear dissemination and discussion of matters relating to information governance; the provision of management information; and proposed system developments with key stakeholder groups.

ii. Reporting
   a. The group meets termly with minutes of each meeting provided via the chair to the University's Directorate function.

III. Information Governance Board

i. Responsibilities
   a. To oversee and assure the implementation of the Information Strategy, the quality of the University's information governance procedures and the continued enhancement of information services, systems and associated administrative processes.
   b. To review and revise the University's information governance policies, in particular the University's compliance with General Data Protection Regulations (GDPR).
   c. To scrutinise and recommend for approval projects consistent with the University's Information Strategy including those related to; data capture and quality, information governance and system developments.
   d. To oversee the risk profile associated with the Information Strategy and associated information owners, systems and data sets.
   e. To prioritise, resource and monitor the planned development and support of the University's information management processes and systems.
   f. To oversee, audit and assure the quality of the University's internal data sets.
   g. To contribute to the annual review of the Information Strategy including issues relating to data quality, integrity, security and regulation.

ii. Reporting
   a. The group meets bi-monthly with minutes of the meeting provided to the University's Information Strategy Group.

IV. Information Governance Office

i. Responsibilities
   a. To oversee the University's information governance function including the compilation, publication and review of the Information Strategy and associated policies.
   b. To provide a centralised function for the management of DP1 requests.
   c. To manage operational issues relating to GDPR and FOI requests.
   d. To take an overview of the University's data structures and data flows with a view to advising on effective management thereof.
   e. To provide training and guidance on data management functions, in particular in relation to legal compliance.
   f. To author, coordinate and approve the implementation of all Data Sharing Agreements.

ii. Reporting
   a. Any incidents giving rise to breaches in information governance legislation are reported to the University's Directorate team.
   b. Sensitive FOI requests are discussed with the University's Directorate on a needs basis.
   c. Termly reports to the Information Governance Board are produced to show progress against core project streams and to highlight any areas of concern or best practice.
   d. Annual reports to the Information Governance Board will provide a summary of all activity including the volume of requests received against the relevant legislation.

e. The Information Governance Office will be required to update the University Data Protection Officer on any areas of concern.

V. IT Services

iii. Responsibilities

a. To ensure University IT infrastructure is robust and secure.
b. To plan, manage and maintain the IT infrastructure to ensure that adequate processing power, storage and network capacity are available for current and projected University needs.
c. To provide support and guidance to University staff regarding IT security.
d. To ensure IT systems are used in line with the University's IT Acceptable Use and Information Security policies.
e. To report any breaches of the University's IT Infrastructure to the University's Directorate.
f. To provide support, guidance and insight in respect to data management and information security requirements.

iv. Reporting

a. Staff have a duty to report any issues as required via the line management system.
b. Reports relating to changes in the IT infrastructure are reported on a termly basis to the Information Strategy Group.

VI. Line Management

i. Responsibilities

a. To be responsible for implementing the information governance policies within their business area, and for adherence by their staff.
b. To assign generic and specific responsibilities for information governance and records management – namely Information Asset Owners and Local Information / Data Managers.
c. To liaise with the Information Governance Board with respect to the application of all appropriate policies including those related to records retention, the transfer and disposal arrangements for records for their areas of responsibility.
d. To ensure that all staff in their business areas undertake relevant training provided by the University and are aware of their accountability for information governance.
e. To ensure that the University's information assets, systems and business applications will be accessed by suitably trained and qualified staff.
f. To assign generic and specific responsibilities for IT applications, systems and services managed within their business area – namely System Owners and System Managers.
g. To ensure designated System Owners / System Managers administer and maintain:
    - System roles, user management and access rights for local applications and information assets to ensure that approved users have access only to such information as is necessary to fulfil their duties.

- Documentation relating to system planning, change control procedures (and approvals), and user acceptance testing.
- Departmental Business Continuity Plans (BCPs) to manage the risks associated with local information assets, operations, systems and business activities.

h. To ensure that responsible staff liaise with University IT Services staff and the Information Governance Office to apply agreed information governance, records management, archive processes, user and system management controls, and information security policies.

i. To ensure that any owned information assets and data sets are secured and shared in line with the University's policies, and that an accurate and timely record of these are maintained within the University Information Asset Register.

ii. Reporting

a. Line Managers have a duty to report any breaches in the University's Information Governance procedures, IT Acceptable Use or Information Security policies to the Information Governance Office providing details of the breach and any actions taken to rectify the issue.

VII. Individuals

i. Responsibilities

a. To maintain accurate and reliable records in line with their roles and responsibilities.

b. To apply good housekeeping principles; by using naming conventions and version control, following filing procedures and saving relevant emails to shared information systems to ensure that in their absence, other colleagues with a requirement to do so can readily find the right information.

c. To follow the University's IT Acceptable Use and Information Security policies and procedures to protect records containing personal data and other confidential information from unauthorised access.

d. To work with their managers and colleagues to apply the records retention policies relevant to their work; so that records are kept locally only as long as required and then securely destroyed or transferred for longer term storage or archival preservation.

e. To undertake relevant training and awareness activities provided by the University to support compliance with this policy.

ii. Reporting

a. Individual have a duty to report any breaches in the University's IT Acceptable Use and Information Security policies to the Information Governance Office and their line manager, providing details of the breach and any actions taken to rectify the issue.

Risk Management

Risks arising from poor information governance practices should be highlighted via the University's risk management process. Sources of immediate risk should be reported to the University's Information Governance Office.