Information Governance Policy

Document Title: Information Governance Policy			
Version No.	1.0	Policy Owner	LGS
Superseded version	N/A	Author Role Title	Head of Information Governance
Approval Date	18.05.2021	Approved by	UET
Effective Date	**18.05.2021**	Review Date	June 2022

1. Introduction

.

1.1 Information governance is an accountability and decision-making framework which ensures that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximise operational efficiency. It includes the processes, roles, policies and standards that ensure the compliant and effective use of information in enabling an organisation to achieve its goals. The University's Information Governance Framework is at Appendix A.

1.2 The regulatory, reputational and operational risks of poor information governance are ever increasing. As the creation of information proliferates, it is vital that the University has measures in place to manage and control these risks. The management and use of information is key to achieving the University's wider aims.

2. Purpose of Policy/Document

2.1 This Policy establishes the key high-level principles of Information Governance at the University and sets out responsibilities and reporting lines for members of staff. It provides an over-arching framework for Information Governance across the University.

3. Scope

3.1 This Policy applies to all users of University information and information systems, including staff, students, authorised third parties and the University's subsidiary companies. It covers information of all types, including personal and none-personal data, in all formats whether electronic or hard copy and any hardware or software used to process it, including the University computer network.

4. Policy Statement

4.1 The governance of information and records management is a core corporate function. The University is committed to the identification of information and business systems that hold records and provision of the resources needed to maintain and protect the integrity of those systems and the information they contain.

4.2 The University's Information Governance Framework is designed to ensure compliance with various pieces of legislation relating to the handling and use of information, as well as the common law duty of confidentiality. These include, but are not limited to:

4.2.1 Data Protection Act 2018
4.2.2 General Data Protection Regulation (EU) 2016/679
4.2.3 Freedom of Information Act 2000
4.2.4 Privacy and Electronic Communications (EC Directive) Regulations 2003
4.2.5 Environmental Information Regulations 2004
4.2.6 Human Rights Act 1988
4.2.7 Limitation Act 1980

A guide to key Information Governance Legislation is at Appendix B

4.3 There are also non-legislative compliance requirements that the University must adhere to such as the Payment Card Industry Data Security Standard (PCI DSS).

4.4 Information Governance is part of the corporate risk management framework and is to be considered when planning or implementing new systems, when extending staff access to new technologies and during re-structuring or major changes to the business so as to reduce risk to the University.

4.5 The University will ensure relevant training is in place to assist staff in their day to day handling of information. All new staff must complete the University's mandatory Information Security & Governance and Data Protection training programmes to ensure they are aware of the risks and their responsibilities in handling information. Staff will be required to complete refresher training [bi-annually] reflecting any changes and updates in information governance best practice.

5. Roles & Responsibilities

5.1 There are a number of key roles and responsibilities across the University in relation to information governance, as set out below. The framework diagram at Appendix C details the relationships between the various roles.

5.2 The Information Governance Project Board ("IGPB") will be the primary forum for discussions relating to information issues across the University and its membership will include staff from the relevant parts of the

University where information issues are of prominence. The terms of reference for IGPB set out the membership and remit of the group.

5.3 The Information Governance Project Team is a group of Information Governance Champions who play an important role in cascading Information Governance knowledge throughout the University's Teams and Schools and who are responsible for providing assurance in relation to the handling of information in their respective areas.

5.4 All staff, including honorary staff/associates, contractors, hourly paid staff and any students who are carrying out work on behalf of the University (including internships), are responsible for ensuring that they are aware of the requirements of the University's policies in relation to information governance and adhere to them on a day to day basis.

5.5 All staff are responsible for highlighting areas of perceived risk where information practices could be improved and to report any incidents that could be considered a breach of the University's internal policies or external legislation.

6. Policy Enforcement – sanctions for non-compliance

6.1 All staff will be required to enter into confidentiality obligations with the University and to participate in information governance training during induction and periodically throughout their employment or engagement. Any breach of confidentiality and/or the University's information governance policies may be a contractual and/or disciplinary matter which could result in termination of an individual's employment or engagement by the University.

7. Related Documents

7.1 The University has a number of related policies which are relevant to this policy. These include:

7.1.1 Data Protection Policy
7.1.2 Data Protection Code of Practice
7.1.3 Data Breach Management Policy
7.1.4 Privacy & Monitoring Policy
7.1.5 CCTV Policy
7.1.6 Criminal Convictions Policy
7.1.7 Appropriate Policy Document (as required by Data Protection Act 2018)
7.1.8 Information Security Policy
7.1.9 Freedom of Information Policy

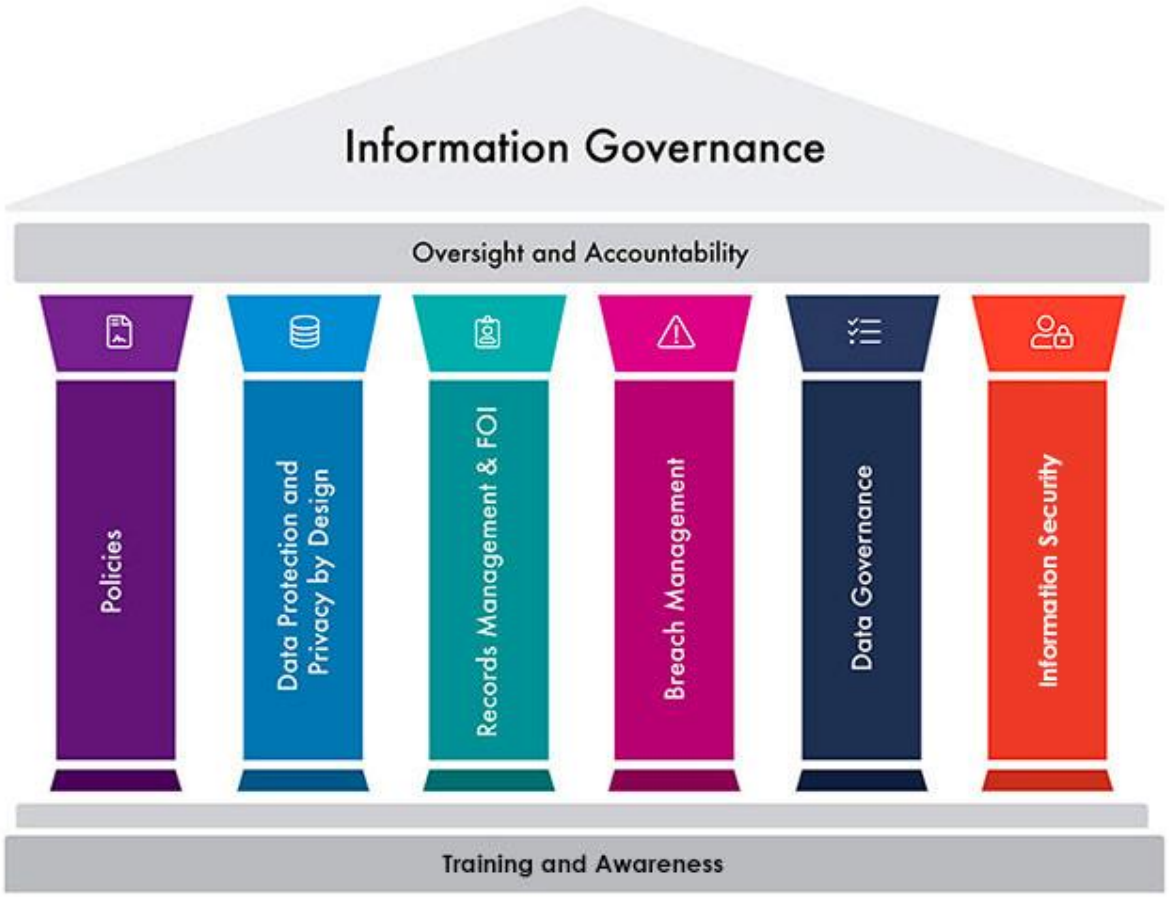
7.1.10 Records Management Policy
7.1.11 Research Data Management Policy
7.1.12 Classification Policy
7.1.13 Records and Retention Policy
7.1.14 IT Acceptable Use Policy
7.1.15 Remote Working Policy

8. Dissemination and Communication Plan

8.1 This Policy will be disseminated by Metacompliance and will be maintained on the University Policy Repository.

Appendix A

Information Governance Framework



Appendix B

Guide to key legislation relevant to Information Governance

Introduction

There are a number of pieces of legislation relevant to Information Governance that must be adhered to if the University is to remain legally compliant when using, storing and handling information. A summary of the main pieces of UK legislation are below.

The General Data Protection Regulation and Data Protection Act 2018

https://gdpr-info.eu/
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The General Data Protection Regulation and Data Protection Act regulates the use of personal data by organisations. Personal data is defined as information relating to a living, identifiable individual.

The legislation is underpinned by eight guiding principles:

1. Personal data shall be processed fairly and lawfully (lawfulness fairness and transparency).

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (purpose limitation).

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed (data minimisation).

4. Personal data shall be accurate and, where necessary, kept up to date (accuracy).

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes (storage limitation).

6. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (integrity and confidentiality).

The Data Controller needs to be able to demonstrate compliance with the above (the Accountability principle)

The Information Commissioner has the power to issue fines of up to €20 million or 4% of turnover for a breach of the Data Protection Act.

Freedom of Information Act 2000

http://www.legislation.gov.uk/ukpga/2000/36/contents

The Freedom of Information Act gives individuals a right of access to information held by the University, subject to a number of exemptions. Requests for information must be made in writing (email, letter or fax) but can be received by any member of staff at the University. Such requests must be responded to within 20 working days. The University has an internal appeal process if a requester is unhappy with a response to a request and the Information Commissioner regulates the Act.

Privacy and Electronic Communications Regulations 2003

http://www.legislation.gov.uk/uksi/2003/2426/contents/made

Section 11 of the Data Protection Act allows individuals to control the direct marketing information they receive from organisations. The Privacy and Electronic Communications Regulations specifically regulate the use of electronic communications (email, SMS text, cold calls) as a form of marketing and allow individuals to prevent further contact.

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

The Human Rights Act puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's "private and family life, his home and his correspondence", a right that is also embedded within the Data Protection Act.

Limitation Act 1980

http://www.legislation.gov.uk/ukpga/1980/58

The Limitation Act is a statute of limitations providing legal timescales within which action may be taken for breaches of the law – for example, six years is the period in which an individual has the opportunity to bring an action for breach of contract. These statutory retention periods will inform parts of the University's records management policy.

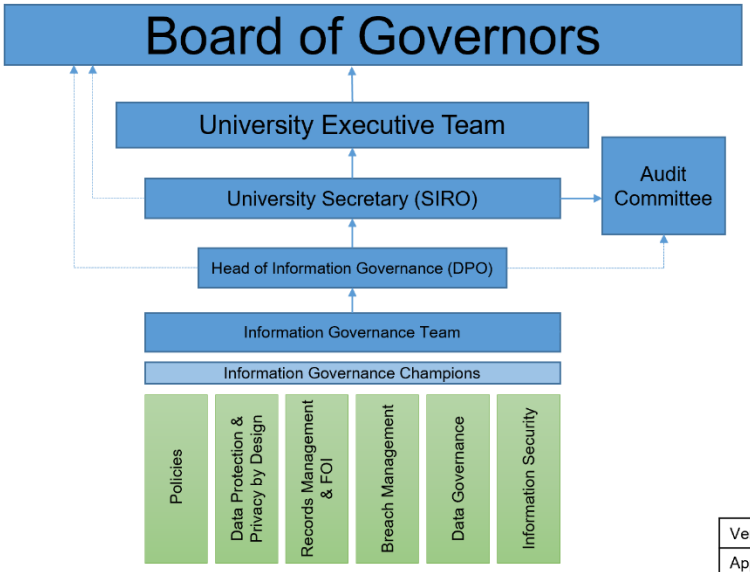
Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

http://www.legislation.gov.uk/uksi/2011/1208/contents/made

An amendment to the Privacy and Electronic Communications Regulations in 2011 obliged websites to inform users about their use of cookies and seek consent for setting more privacy intrusive cookies.

Appendix C

Information Governance Accountability Structure



Version	1.0
Approval Date	09/12/2020
Approval route	IGFP Board

Equality and Prevent Impact Assessment (V1.2)

Proposal Title		Key aims & purpose
Contact name & details of Policy Owner/Sponsor	Name: Kate Heljula	**Assessment date:** 18.03.21
	Phone:	
	Email: k.heljula@tees.ac.uk	

To comply with the Equality Act 2010 we are required to consider the possible consequences of decisions the University makes on people from different groups. ***For more information about the Equality Act follow this link:***
http://www.ecu.ac.uk/wp-content/uploads/external/psed-specific-duties-for-england-sept11.pdf

		Yes	No	Notes
1.	Is it a major policy, significantly affecting how functions are delivered?			
.	Is it likely that this proposal will disproportionately affect people who have protected characteristics (*age, disability, gender reassignment, religion and belief, race, sex, sexual orientation, pregnancy and maternity and marriage and civil partnership)* who are employees, students, service users or other stakeholders, or the wider community?		x	
	Have there been any reported issues or complaints about this policy in relation to any particular protected characteristics?			
2.	**Could this proposal support the university to meet the following three requirements of the Public Sector Equality Duty?**			
	a) Does it support the University to…*eliminate discrimination, harassment, victimisation and any other conduct that is prohibited under the Equality Act 2010?*	x		
	b) Does it enable the University to…*advance equality of opportunity between different groups of people?*	x		

	c) Does it help the University to…*foster good relations between different groups of people?*	x		

To comply with the Counter-Terrorism and Security Act 2015 Universities are under a legal duty to prevent people from being drawn into terrorism ("Prevent"). *For further information about the duty follow this link:*
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445916/Prevent_Duty_Guidance_For_Higher_Education__England__Wales_.pdf

		Yes	No	Notes
3.	Could this proposal contain or increase risks that people may be drawn into terrorism?		X	
	Could the proposal have any other impact on the University's ability to comply with its duty under Prevent to have due regard to the need to prevent people from being drawn into terrorism?		X	
	Is a separate risk assessment required?		X	
	Is the proposal likely to contain any Safeguarding implications that could result or be impacted by the proposal?		X	
	Is a separate risk assessment required?		X	
4.	**Equality Assessor Recommendations and Notes:** The policy expressly recognizes and promotes the need to avoid discrimination in the provision of student references.			
5.	**Please select an outcome:**		✓	**Notes**
	a) No major change to is required:			

	b) The proposal will be adjusted (as above) and submitted for decision:	
	c) The proposal will be continued without change and monitored.	
	d) The activity will be stopped and the policy will be removed:	
	e) Further assessment is required:	
6.	**Signed by Equality Assessor _____ Date:_____**	