University of Sunderland – Business Assurance

Over-arching Information Governance Policy

Document Classification: **Public**

Policy Reference – Central Register	IG001_____
Policy Reference – Faculty / Service	IG 001
Policy Owner	Director of Business Assurance
Date Policy Written	May 2013
Date Policy Last Updated	May 2016
Author	Assurance Manager, Business Assurance
Date to Information Governance Group	June 2016
Date to Executive	
Date for next Review	June 2017
Updates from Previous Version	Purpose and Scope updated Inclusion of Incident Management and updated list of policies

Contents

Over-arching Information Governance Policy

1. Introduction

Information Governance is the term used to encompass the multi-disciplinary structures, policies, procedures, process and controls which are implemented to manage the processing of information within an organisation. It provides a framework for processing information in a confidential and secure manner, as determined by legislative acts, statutes and best practice guidance.

2. Purpose and Scope

This policy applies to all staff of the University and its subsidiary companies and independent contractors. It applies to all information, in all formats.

The purpose of this document is to provide a framework for the handling of information in the University to ensure regulatory and statutory compliance and to ensure that appropriate use of timely and accurate information assists in the delivery of the University's Strategic Objectives.

3. Aims and Objectives

Through effective information governance, the University aims to:

- Provide timely access to accurate, relevant information
- Achieve a defensible disposition
- Ensure compliance with legislation and good practice
- Reduce information risk through consideration of defensible disposal regime
- Realise the value of good information
- Improve security of information
- Improve collaboration between partner agencies
- Rationalise processes and increase their effectiveness
- Increase employee productivity
- Decrease storage wastage
- Improve resilience and ensure business continuity

4. Information Governance Responsibilities

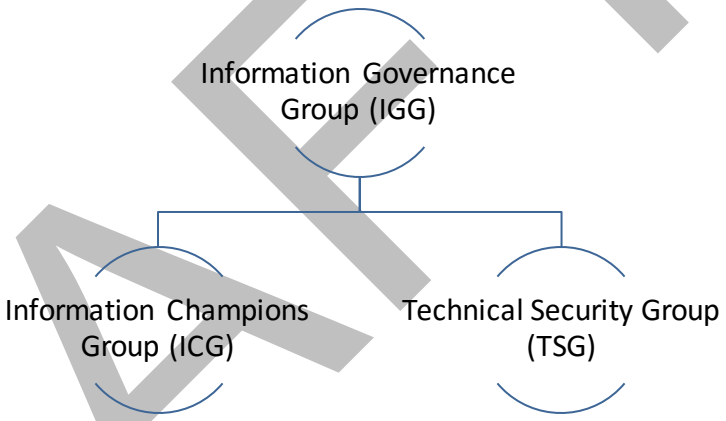
All individual employees and contractors have responsibility for ensuring that they comply with this policy and any related policies and guidance and to report any incidents or 'near misses' in relation to information security.

The University has identified the following roles in relation to Information Governance:

Role	Responsibility
Board of Governors and Vice Chancellor	Ultimate responsibility information governance rests with the Board of Governors. The Vice Chancellor, has executive responsibility for all aspects of information governance and together with the Board of Governors, will ensure that proper procedures are in place to fully implement this policy. The Vice Chancellor is also responsible for signing any undertakings issued by the Information Commissioner due to non-compliance.
Senior Information Risk Owner (SIRO)	Overall responsibility for this policy lies with the Director of Business Assurance, who performs the role of the University's Senior Information Risk Owner (SIRO) The SIRO is responsible for: Ensuring that an overall culture exists that values and protects information within the organisation • Owning the organisation's overall information risk policy and risk assessment process, testing its outcome and ensuring that it is used • Owning the organisation's information incident management framework
The Assurance Manager (Information Governance)	The Assurance Manager, responsible to the Director for Business Assurance, is responsible for drawing up information governance policy, process and guidance and ensuring compliance with this policy. The Assurance Manager will oversee the Information Governance Framework and ensure its successful operation.
IT Services	IT Services are responsible for delivering a business led cyber security architecture, IT operations management and obtaining, monitoring and acting on vulnerability information, ensuring a proportionate response to actual, suspected or imminent breaches in IT security.
Legal Support and Data Protection Officer	The Legal Support and Data Protection Officer is responsible for developing policy, process and guidance relating to Data Protection and providing advice on collecting, using and protecting personal information.
Information Asset Owners	Information Asset Owners are responsible for maintaining a register of information assets under their ownership and associated risks.
University Deans of Faculty and Directors of Support Services	The University Deans and Directors have responsibility for ensuring compliance with the University's Information Governance policies and ensuring any issues of non-compliance are addressed. They have responsibility for ensuring that an appropriate member of staff, in each Faculty and Service, takes on the role of "Information Champion".

5. Governance Groups

The following groups have been established within the University:



Role	Responsibility
Information Governance Group	The Information Governance Group is accountable to the University's Business Assurance Board. It is to act as a programme board for direction of the University's overall approach to Information Governance. Specifically, it is tasked with:- • Holding an understanding of all elements of Information Governance, including relevant technical and legal requirements • Overseeing all aspects of policy development in relation to Information Governance, including the approval of policies • Overseeing all technical developments to support and enhance the University's approach to the management of Information Governance • Governing the design and delivery of all training and development activity in relation to Information Governance
Information Champions Group	Information Champions are accountable to their Dean of Faculty/Director of Service and have a responsibility to monitor information governance compliance and awareness and be the primary point of contact and source of information and support within the Faculty/Service. The Information Champions Group will report to the Information Governance Group.
Technical Security Group	Faculty IT Technicians play a pivotal role in the application of technical IT Security controls within their Faculty and are accountable to their Dean of Faculty/Director of Service for ensuring the IT Services provided by the Faculty are in line with IT Security Policies & Standards. The technicians must also be a primary point of contact and source of information in relation to IT Security form an awareness perspective in supporting the Faculty/Service. The Technical Security Group will report to the Information Governance Group.

6. Policies and Procedures

The University will implement information governance policies and procedures which are embedded in day to day operations and which are compliant with relevant legislation, standards and codes of practice and demonstrate good practice.

Policies and procedures will be implemented in the areas of:

6.1. Confidentiality and Data Protection

The obligation to keep information confidential arises out of the common law duty of confidentiality, the Data Protection Act 1998, professional obligations and staff employment contracts. In combination, these duties and obligations place all staff members with access to confidential personal information under a duty to keep that information safe and secure

6.2. Information Security and Information Risk Management

The aim of information security is to prevent loss, damage or compromise of assets and interruption to business activities.

The main priorities for information security are:

- creating a culture towards information security within the organisation
- ensuring security policies contain sufficient detail and strength to guide staff
- ensuring staff have access to policies and guidance and sufficient training to ensure they can fulfil their duties responsibly and securely
- developing IT Security standards and technical best practice guidance documents to be implemented across the organisation

6.3. Records Management

Good records management helps to ensure that records are accessible and retrievable when and where required. This includes records on network drives, emails and attachments, web pages on Internet and Intranet sites and paper records held both off-site and on-site. Records management will concentrate on themes such as:

- Creating and maintaining an inventory of existing corporate records
- Creation/File Naming conventions
- Information classification
- Storage
- Retention periods
- Archiving
- Disposal
- Compliance with legislation such as Freedom of Information Act /Environmental Information Regulations
- Electronic document management including use of 'cloud –based' services
- Corporate records management (including policy management)
- Open access to outputs of publicly funded research

6.4. Incident Management

An information governance incident can be any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1981 and/or the Common Law of Confidentiality.

This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.

Such personal data breaches which could lead to identity fraud or have other significant impact on individuals.

Incidents may be caused through, for example:

- Information being lost in transit;
- Information being lost or stolen;
- Information being disclosed in error through mis-directed e-mails and letters;
- Unauthorised access to systems.

6.5. Training and Awareness

Information is the lifeblood of the University. It is essential that a culture is developed whereby information management is part of everyday activities and becomes part of the culture of the organisation. Increasing staff awareness is key to successfully implementing a University-wide approach to Information Governance. Training and awareness will be available to all staff, dependent upon job role and will be deployed using a variety of techniques including:

- e-learning
- face to face training sessions
- facilitated workshops
- external training providers

7. Relevant Legislation and Good Practice

7.1. Regulatory Environment

Relevant legislation includes:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- Human Rights Act 1998
- Access to Health Records Act 1990
- Lawful Business Practice Regulations 2000
- Mental Capacity Act 2005
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)

7.2. Best Practice

Related guidance and codes of good practice:

- Security Policy Framework (Cabinet Office).
- Public Service Network (PSN) Code of Connection.
- The ICO's published guidance and codes of practice
- NHS IG Toolkit
- SANS Institute
- ISO Standards
- Cyber Essentials Scheme

APPENDIX A – OVERVIEW OF INFORMATION GOVERNANCE POLICIES

General	Records Management	Data Protection/Confidentiality	Information Security (and related policies)
Over-arching Information Governance Policy	Records Management Policy	Data Protection Policy	Information Security Policy
Data Assurance Policy	Archive and Retention Policy	SAR Procedures	IT Acceptable Use Policy
Using Copyright in Education	Information Classification Policy	Staff Guide to Personal Information	IT Security Policy (and standards)
Information Governance Training Policy	Archiving and Retention Procedures	Student Guide to Personal Information	Information Risk Management Policy (and procedures)
	FOI and EIR Policy	Data Sharing Agreement Guidance	JANET Acceptable Use Policy
	FOI Procedures	Non – disclosure Agreement Guidance	Business Continuity Policy
	Data Quality Policy		PCI Security Policy
			Interception and Monitoring Policy
			Incident Management Policy