Overarching Information Governance & Security policy

(Version 4)

Version:	**4**
Dated:	**01 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
2.4	n/a	P Sandy/ D Waymouth	n/a
3.0	Dec 2015	C Dominey	Reformatting and Minor amendments
3.1	May 2018	R Platt	Updated to reflect GDPR and IG framework
4	May 2018	R Platt	ApprovedVersion

Approval

Version	Approval Board	Date of Approval
3.0	Interim Chair of ISSG & Head of Governance and Compliance	Dec 2015
4.0	Information Governance & Security Steering Group	May 2018

1 Introduction

Information Governance is a framework to bring together all the requirements, standards and best practice that apply to the handling of information. It allows the University and individuals to ensure that information is accurate, dealt with legally, securely, efficiently and to deliver the best possible service.

Information is a vital asset, enabling the University to deliver world class education and research and the efficient management of services and resources.

It is therefore of paramount importance that information is efficiently managed and that appropriate policies, procedures and management accountability are in place. This will provide a robust governance framework for information management across the University.

This policy and its subsidiary policies aim to ensure that information stored and processed by the University, or on behalf of the University, across all University activities, in any form and any location is securely protected against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

2 Scope

This policy and its subsidiary policies apply to all information that is owned, stored or processed by the University or on behalf of the University.

They apply to IT systems that hold University data whether these are in house, off site or developed by a third party. Information includes information stored and processed though computerised information systems and on paper or in any other form such as photographs. It includes information held on laptops and other mobile devices such as USB memory sticks. They apply to any storage, processing or use of information on and off campus, including working at home, while travelling and at partner organisations

All employees, workers, students, contractors and other relevant parties have a responsibility to comply fully with this policy, and any specific subsidiary information security policies and standards issued to support it.

3 Roles and Responsibilities

3.1 Information Governance & Security Steering Group (IGSSG)

The Information Governance & Security Steering Group is responsible for the strategic, senior management overview and the direction of information governance and security across the University. The IGSSG is chaired by the SIRO and reports, via the SIRO, to the Vice-Chancellor's Executive Group.

3.2 The Senior Information Risk Owner (SIRO)

The University of Exeter's Senior Information Risk Owner (SIRO) is the Registrar and Secretary. He is the member of the Vice-Chancellor's Executive Group with overall responsibility for the University's information risk policy. The SIRO is accountable and responsible for information risk across the University and for sponsoring and promoting information governance policy.

3.3 Senior Information Officers (SIO)

Directors of College Operations and Directors of Professional Service are responsible for overseeing compliance with these policies and relevant legislation within their designated area to ensure the protection of information and that appropriate information governance and security processes are implemented in their College / Service. College and Service management teams will consider information governance and security on at least a quarterly basis. Each College, Service and partner organisation will designate a lead person for ensuring the development, communication and implementation of

information governance and security in their College / Service / organisation. SIOs will support the University's SIRO in his overall information risk management function.

3.4 **Information Asset Owners (IAO)**
IAOs are accountable for ensuring their information assets are identified and compliant with this and all subsidiary policies and relevant legislation. IAOs will support the University's SIRO in his overall information risk management function.

3.5 **System Owners**
System owners are not all within Exeter IT. They are responsible for ensuring their systems are compliant with this policy and all subsidiary policies and information is managed and secured to the level as defined by the IAO.

3.6 **Information Governance Manager**
The Information Governance Manager is responsible for leading the University's information governance strategy, policies and procedures covering all elements of information governance (including information security, data protection, freedom of information and information management). As the Data Protection Officer, she has responsibilities as defined by the General Data Protection Regulation.

3.7 **Exeter IT – Head of IT Security & Compliance; Operations & Security Manager**
The Head of IT Security & Compliance and the Operations & Security Manager are responsible for leading and delivering the University's technical information security governance, compliance and capability.

3.8 **Managers and Supervisory roles**
All employees in managerial or supervisory roles have the responsibility of overseeing compliance with this and all subsidiary policies and relevant legislation and developing good practice within their designated areas.

4 Policy

4.1 Data Protection Impact Assessments will be undertaken to identify the probability and impact of security failures and to determine the appropriate security measures to be applied to information.

4.2 The University will maintain an information asset register.

4.3 All identified or suspected data breaches or incidents must be reported in line with the University's Data Breach Policy.

4.4 All staff must undertake the mandatory online Information Governance training course. PGRs and associates (including temporary staff) may be required to undertake the course where relevant to their role.

4.5 Subsidiary information security policies for specific activities and systems, which support the management framework of this policy and include details of technical control measures, will be maintained, communicated and implemented.

4.6 Specialist advice on information governance and security is provided through the Information Governance Team within Compliance, Governance & Risk and through IT Security & Compliance and Operations & Security within Exeter IT, who together support overall implementation of information governance and security policy across the University.

4.7 Procurement arrangements will take account of information governance and security requirements.

4.8 This policy and specific subsidiary information governance and security policies, standards and arrangements issued to support it will be regularly reviewed and audited by third parties.

4.9 Monitoring, enforcement and (where necessary) interception will be used to ensure compliance with the University's information security policies.

4.10 The University will adopt a standards-based framework for information security and will use the BS ISO / IEC 27000 Information Security Standard suite of documentation, with a view to possible future accreditation.

4.11 This policy will be regularly reviewed by the Information Governance & Security Steering Group to ensure that it remains appropriate in the light of any relevant changes to the law, University policies, contractual obligations, technological developments and emerging threats.