

Information Governance Policy

From: Chief Information Officer

Date: September 2017

1 Introduction

- 1.1 Information is a vital asset that underpins the University's research, teaching and enterprise. Information governance is the process by which the handling of that organisational information is managed and controlled, in particular, the personal and sensitive information of University staff, students, agency staff, patients, visitors, contractors and third parties (Users).
- 1.2 The University recognises the need to maintain a balance in its management and use of information between:
 - 1.2.1 its public accountability and transparency in its governance,
 - 1.2.2 its compliance with legal and regulatory obligations and
 - 1.2.3 the need to both protect and secure the personal and commercially sensitive information that it has responsibility for.
- 1.3 A framework of information governance and security policies, procedures and controls have been developed to manage information in a cohesive way to ensure that all information, including personal information, is dealt with legally, securely and effectively so that all Users who have access to that information know what information is held, where it is held, who is responsible for it and how long it is kept.
- 1.4 This framework implements appropriate technical and organisational measures that ensure and demonstrate that the University is complying with its obligations under General Data Protection Regulations (EU) 2016/679).
- 1.5 It is intended that the University will engage in upskilling all Users proportionate with their key user obligations. The Chief Information Officer, as SIRO, shall, from time to time, determine the roles for which this requirement will be considered mandatory.

2 Scope

- 2.1 This policy applies to all Users and the University's partner organisations that have responsibility for the collection, use, maintenance and disposal of University information.

3 Aims

- 3.1 The University's information is used as the basis on which decisions are made and services provided. The aim of information governance is to ensure that this information, whether in paper or electronic format, is handled efficiently and effectively at all times. In particular, information governance should help to:
- 3.1.1 Maintain confidence in the reliability of information;
 - 3.1.2 Protect the privacy of Users;
 - 3.1.3 Provide effective and efficient services to Users;
 - 3.1.4 Support decision-making by ensuring that relevant, accurate and comprehensive information is readily available to inform the future of the University;
 - 3.1.5 Ensure accurate funding allocations and demonstrate accountability to public and private funders;
 - 3.1.6 Increase cost-effectiveness by making sure data is disposed of when no longer needed;
 - 3.1.7 Minimise the risk of information security breaches; and
 - 3.1.8 Ensure the University's compliance with legal and regulatory requirements.

4 Monitoring compliance and review

- 4.1 All information governance and security policies and procedures will be subject to periodic audit and review to ensure that they remain fit for purpose and the University remain compliant.

5 Roles and responsibilities

- 5.1 Key Roles and Responsibilities are attached at Schedule 1.

6 Key information governance policies and guidance

- 6.1 Key legislation is the Data Protection Act 1998, the Data Protection Bill 2017 and the General Data Protection Regulations (EU) 2016/679).

6.2 Key Information Governance policies and guidance are set out in the Information Governance Framework at:

<https://intranet.soton.ac.uk/sites/gdpr/Pages/Home.aspx>

7 Further information

7.1 Further advice and support can be found at:

<https://intranet.soton.ac.uk/sites/gdpr/Pages/Home.aspx>

7.2 We also have additional policies and guidelines concerning particular activities. Please see our Publication Scheme at:

https://www.southampton.ac.uk/about/governance/regulations-policies-guidelines.page#publication_scheme

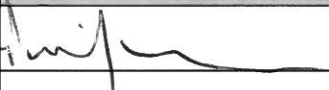
Document Control

File Name	Information Governance Policy
Original Author(s)	FTVB
Current Revision Author(s)	FTVB
Owner	Chief Information Officer
Publication Date	
Target Audience	

Version History

Version	Date	Author(s)	Notes on Revisions
00.1	May 2015	FTVB	
00.2	December 2016	FTVB	
00.3	May 2017	FTVB	
00.4	Sept 2017	FTVB	Incorporating amends from IGG

Document Sign Off

Name	Role	Doc version	Signoff date	Signature*
Ian Dunn	COO		08/12/2017	

*If signoffs are received by email, print names here and archive the sign off emails.
Add location of signoff emails here:

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Intranet is the controlled document copy. Any printed copies of this document are not controlled.

Schedule 1 Roles and Responsibilities

1 Chief Operating Officer (“COO”) will:

- 1.1 Understand the strategic business goals of the University and how they may be impacted by information risks, and how those risks may be managed.
- 1.2 Be responsible for reporting to the University's governing body via the audit Committee.

2 Chief Information Officer (“CIO”) will:

- 2.1 Undertake the role of Senior Information Risk Owner (“SIRO”) and will receive training as necessary to ensure that they remain effective in their role as SIRO.
- 2.2 Understand the operational business goals of the University and how they may be impacted by information risks, and how those risks may be managed.
- 2.3 Chair the Information Governance Group.
- 2.4 Advise the Information Governance Group on the effectiveness of information risk management.
- 2.5 Implement and lead the University information governance risk assessment and management processes.
- 2.6 Act as champion for information risk on the Information Governance Group and provide written advice on the content of the University's statement of internal control in regard to information risk.
- 2.7 Have overall responsibility for establishing an effective electronic and paper document management system.
- 2.8 Have overall responsibility for the University's Information Governance Policy, ensuring this remains aligned with legal and regulatory requirements.
- 2.9 Report to the COO and the Information Governance Group on information governance and incident reporting, where appropriate.
- 2.10 Provide reports on incident numbers, trends and themes information security incidents and issues to the Audit Committee.

3 Data Protection Officer (DPO) will:

- 3.1 Inform and advise the University and its employees about their obligations to comply with the Data Protection Act 1998 (DPA), the General Data Protection Regulations (GDPR) and other data protection laws.

- 3.2 Monitor compliance with the DPA and the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments and maintain a data protection asset register; train staff and conduct internal audits.
- 3.3 Will be the first point of contact for lead supervisory authorities and for individuals whose data is processed.

4 Information Governance Group (“IGG”) will:

- 4.1 Consist of the Chief Information Officer as SIRO, Chief Operating Officer, Head of Information Security, Director of Legal Services (in own right and in capacity as Data Protection Officer), Director of Library Services, Executive Director of Engagement and Advancement, Director of iSolutions, a nominated representative of the Senior Academic Team and of the Heads of Faculty Operations, and any other person who from time to time the Chief Information Officer feels it is appropriate to include.
- 4.2 Ensure the development of effective policies and management arrangements covering all aspects of Information Governance and security where appropriate.
- 4.3 Maintain oversight of and promote the accuracy and consistency of information presented by the University through its published channels.
- 4.4 Promote the understanding of and development of best practice in information governance and security across the University.
- 4.5 Receive reports on regular/periodic assessments and audits of information governance and security policies and arrangements and to report on such assessments and audits to the University Audit Committee and Senate and to other committees or groups as required.

5 Head of Information Security will:

- 5.1 Maintain a lead role within the Information Security Management System (ISMS) by identifying risks, maintaining risk treatment plans and providing written or oral summaries on residual levels of risk and the status of corrective actions to iSolutions management or the appropriate University Risk or Information Governance Group.
- 5.2 Conduct investigation, analysis and review following security control breaches, and manage security incidents. Recommend appropriate control improvements, involving other professionals as required.
- 5.3 Monitor the application and compliance of security operations procedures, and report on non-compliance.

6 Information Asset Owners (IAO) will:

- 6.1 Facilitate risk assessments of all appropriate assets.

- 6.2 Identify mitigating actions and review associated risks.
- 6.3 Lead and foster a culture that values and protects information.
- 6.4 Know what information comprises or is associated with the asset.
- 6.5 Understand the nature and justification of information flows to and from the asset.
- 6.6 Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.
- 6.7 Understand and address risks to the asset, and providing assurance to the SIRO.
- 6.8 Ensure there is a legal basis for processing and for any disclosures, and refer queries in regards to any of the above to the Data Protection Officer.

7 Information Asset Custodians will be responsible for:

- 7.1 Supporting in the day to day use and management of information assets in a particular area. They will be appointed by the IAO to have responsibility for overseeing and implementing the necessary safeguards to protect the information assets and report back to the IAO on any changes to risks. The IAO will retain the overall responsibility.

8 Director of iSolutions will also be responsible for:

- 8.1 The formulation and implementation of ICT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust ICT security arrangements in line with best industry practice.
- 8.2 Effective management and security of ICT resources, for example, infrastructure and equipment.
- 8.3 Developing and implementing a robust IT Business Continuity Plan.
- 8.4 Ensuring the maintenance of all firewalls and secure access servers are in place at all times.
- 8.5 Acting as the IAO for the ICT infrastructure with specific accountability for computer and telephone equipment and services that are operated by the University's corporate and clinical work force e.g. personal computers, laptops, personal digital assistants and related computing devices, held as an asset.

9 Deans and Academic Heads will:

- 9.1 Ensure compliance with Data Protection, Information Security and other information related legislation within their Faculty or Academic Unit.
- 9.2 Provide support to those who handle privacy and freedom of information requests.

- 9.3 Report information security incidents to the CIO and/or the Head of Information Security, as appropriate.
- 9.4 Implement University information governance guidance and policy.
- 9.5 Provide support to the CIO in respect of internal information governance and security related issues when requested.
- 9.6 Work with the CIO to ensure there is consistency of information governance across the organisation.

10 Line Managers will:

- 10.1 Be responsible for ensuring that the policy and its supporting standards are maintained in order to achieve full compliance across the whole organisation.

11 All Users will:

- 11.1 Abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance.
- 11.2 Not be able to access information to which they do not have a legitimate access right.
- 11.3 Not knowingly contravene this policy, nor allow others to do so.

12 Caldicott Guardian will: [University of Southampton's Auditory Implant Service ("USAIS")]

- 12.1 Ensure that USAIS satisfies the highest practical standards for handling patient identifiable information.
- 12.2 Facilitate and enable appropriate information sharing and make decisions on behalf of the University following advice on options for the lawful and ethical processing of information, in particular in relation to disclosures.
- 12.3 Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- 12.4 Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies such as the NHS.