Information Governance Policy
(IGP-01)

Summary			
This Policy establishes the key high-level principles of Information Governance at the University of Bristol and sets out responsibilities and reporting lines for members of staff. It provides an over-arching framework for Information Governance across the University.			
Scope			
The Policy applies to all staff employed by the University, including honorary staff/associates, contractors, hourly paid teachers and any students who are carrying out work on behalf of the University (including internships).			
Document Control			
Document type	Information Governance Policy – IGP-01		
Document owner	Information Governance Manager		
Division	University Secretary's Office		
Lead contact	Information Governance Manager		
Document status	Approved		
Version	v2.0		
Approved by	Information Governance and Security Advisory Board & University IT Committee	Date	13/02/2018
Date of publication	July 2018	Next review date	July 2020
Date of original publication	July 2018	Revision frequency	2 years
Superseded documents	N/A		
Related documents	See **Interaction with other policies and procedures** below		

Contents

1. Introduction

Information governance is an accountability and decision making framework put in place to ensure 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.

Information is a key asset for the University and 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 as set out in the Vision and Strategy.

2. Definitions

Information is generally defined as *"knowledge or facts about someone or something"* and *"the communication or reception of knowledge or intelligence"*. It can exist in many different formats but it must have meaning in some context for its receiver. It includes paper-based documents, electronic documents, images, video footage, social media content, statistical or research data, and meta data (being data that are derived from or associated with other data and which describe the characteristics of such data).

Further relevant definitions can be found in Appendix 1.

3. Purpose of this Policy

This policy is intended to set out the high level principles of information governance across the University and to make clear the responsibilities and reporting lines for members of staff. It is intended as an over-arching framework to give clarity about the scope of information governance across the University and to highlight key information and related policies to staff.

4. Scope

This Policy applies to all information held for the purposes of the University's operations including, but not limited to, the provision of teaching and education, research, student and staff support, internal and external reporting and publications. It applies to information created by members of the University and also to information received from third parties.

This Policy applies to all staff employed by the University, including honorary staff/associates, contractors, hourly paid teachers and any students who are carrying out work on behalf of the University (including internships).

5. Roles and responsibilities

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 B details the relationships between the various roles:

Board of Trustees
The Board of Trustees has ultimate responsibility for directing the affairs of the University and, as such, will ensure the University has appropriate information governance procedures in place to mitigate risk and maximise the value of the information it holds.

Senior Information Risk Owner (SIRO)
The SIRO is accountable at a senior management level for ensuring that the University has robust information governance and security processes and procedures in place. This role is held by the University's Registrar and Chief Operating Officer at the accountable executive level, with the Chief Information Officer acting as the responsible person at an operational level.

Information Asset Owners (IAOs)
IAOs are appropriately senior members of staff who have responsibility for specific information assets within divisions or schools. Their role is to ensure those assets are handled and managed properly, that appropriate access and security controls are in place and that the accuracy and integrity of the information is assured. They provide assurance to the SIRO that the information risk is being managed effectively.

Information Asset Administrators (IAAs)
IAAs are members of staff that have been delegated responsibility by an IAO for the operational use of particular information assets within divisions or schools. Their role is to identify and report any operational concerns or risks to IAOs to be escalated accordingly.

Assistant Director IT Services (Governance and Risk)

This role has operational responsibility for ensuring that information governance processes and procedures are in place across the University.

Information Governance Manager
The Information Governance Manager will oversee the information governance framework to ensure that it is operating effectively, and assist the SIRO and IAOs with advice and guidance in relation to the handling and use of information. This role is also responsible for managing the University's Information Asset Register and the University's compliance with the [Data Protection Act/General Data Protection Regulation], Freedom of Information Act and other relevant legislation (as listed in section 5). This role holds the statutory Data Protection Officer role as designated by the Data Protection Regulation.

Information Security Manager
The Information Security Manager has responsibility for ensuring the University has robust information security processes and procedures in place across the University. This role monitors the University's compliance with the Information Security Policy and handles information security incidents, when they arise.

Information Governance and Security Advisory Board (IGSAB)
See section 7.

All staff and third party contractors
All members of University staff, including honorary staff/associates, contractors, hourly paid teachers 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 security and adhere to them on a day to day basis. 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.

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 and security policies may be a contractual and/or disciplinary matter which could result in termination of an individual's employment or engagement by the University.

6. Legal and compliance

The University's information governance framework must 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:

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Computer Misuse Act 1990

- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Malicious Communications Act 1988
- Digital Economy Act 2010
- Intellectual Property Act 2014
- Investigatory Powers Act 2016

Further information about these pieces of legislation is available in the University's guide to information related legislation.

There also other non-legislative compliance requirements the University must adhere to (both internal and external), such as:

- Payment Card Industry Data Security Standard (PCI DSS)
- JANET acceptable use and security policies
- NHS Information Governance Toolkit
- Requirements set out by ethics committees and in line with other regulatory or institutional approvals
- Requirements detailed in contract and funding terms
-

7. Information Governance and Security Advisory Board (IGSAB)

IGSAB 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 IGSAB set out the membership and remit of the group.

8. Records and document management

The Freedom of Information Act Section 46 Code of Practice[1] sets out a number of principles in relation to records management:

- Recognition of records management as a core corporate function;
- Inclusion of records and information management in the corporate risk management framework;
- A governance framework that includes defined roles and lines of responsibility;
- Clearly defined instructions, applying to staff at all levels of the authority, to create, keep and manage records;
- 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;
- Consideration of records management issues when planning or implementing ICT systems, when extending staff access to new technologies and during re-structuring or major changes to the authority;

[1] https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf

- Induction and other training to ensure that all staff are aware of the authority's records management policies, standards, procedures and guidelines and understand their personal responsibilities;
- An agreed programme for managing records;
- Provision of the financial and other resources required to achieve agreed objectives in the records management programme.

The University's Document Management Policy sets out the consistent standards that staff should use when creating, using and disposing of information.

Training

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 training (online) to ensure they are aware of the risks and their responsibilities in handling information. Staff will be required to complete refresher training annually reflecting any changes and updates in information governance best practice.

Information Asset Owners must complete additional training reflecting their role overseeing local procedures in relation to the management and security of information within their remit.

9. Interaction with other policies and procedures

The University has a number of existing policies and procedures that have relevance to information governance, as below, and staff must be aware of their content:

Information Governance Policies:

- IGP-02 - Data Protection Policy
- IGP-03 - Records Management and Retention Policy
- IGP-04 - Records Retention Schedule
- IGP-05 - Document Management Policy
- IGP-06 - Digital Preservation Policy
- IGP-07 - Personal Data Breach Policy
- IGP-08 - Privacy Impact Assessment Policy
- IGP-09 - Information Strategy Principles
- IGP-10 - Information Classification Scheme

Other policies and guidance:

- Information Security Policy
- Information classification scheme
- IT Acceptable Use Policy
- Information Handling Policy
- Mobile and Remote Working Policy
- Outsourcing and Third Party Compliance Policy
- Social Media Policy
- Incident Management Policy / Procedure
- Investigation of Computer Use Policy
- Research Data Management and Open Data Policy
- Open Access to Research Publications Policy

- Guidance on the Retention of Research Records and Data

10. Policy review and ownership

This policy will be reviewed as required and at least every three years by IGSAB. The document is managed by the Information Governance Manager in the Secretary's Office.

Appendix 1: Definitions

Information
Information is generally defined as *"knowledge or facts about someone or something"* and *"the communication or reception of knowledge or intelligence"*. It can exist in many different formats but it must have meaning in some context for its receiver

Documents
ISO9000 defines a document as *"information and its supporting medium",* so it can include a wide range of both hard copy and digital formats, and is not simply limited to written information. Documents can be created in many formats, including (but not limited to):

- Letters (digital and hard copy)
- Emails
- Policies and guidance
- Meeting papers and minutes
- Reports
- Contracts
- Presentations
- Official communications
- Photographs
- Audio recordings

Records
ISO defines records as: *"…information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."* Records are a subset of information and documents.

Information assets
The National Archives[2] defines an information asset as *"a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively".* There are no set rules in defining what an information asset is, but it must be categorised in a way that is understandable and useful to the University and its staff. It can be a single document or a group of related documents.

Information Asset Register
The Information Asset Register documents all the University's information assets, IAOs and associated relevant information. It is managed and updated by the Information Governance Manager on an annual basis.

Document management
The field of management that is responsible for the efficient and systematic control of the creation, distribution, use, maintenance and disposal of documents.

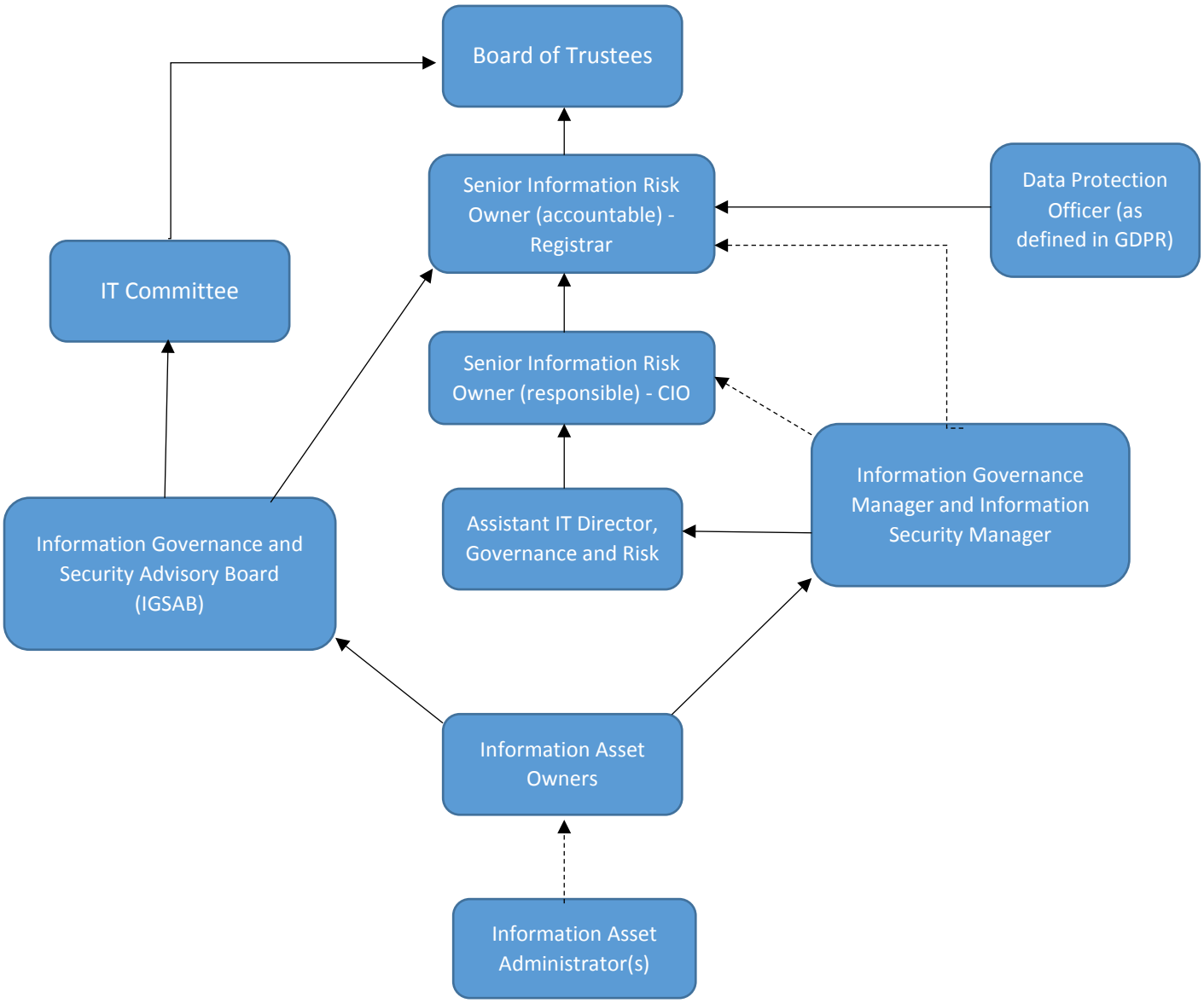
Information Security
The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.

[2] http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

Appendix 2: Information Governance Framework

Direct reporting / communication line

Possible reporting / communication line



Appendix 3: Document history

Version	Author / Primary reviewer	Details of changes	Date	Approved by	Approved date
d0.1 Draft	Information Governance Manager	Initial draft – new policy	Apr 2016		
d0.2 Draft	Information Governance Manager	Incorporating comments from IGSAB	Oct 2016		
v1.0 Approved	Information Governance Manager	Insertion of minor update from IGSAB	Nov 2016	IGSAB	17/11/2016
v1.0 Approved	Information Governance Manager	No changes	Nov 2016	University IT Committee	17/05/2017
v1.1 Approved	External legal review	Minor additions	Feb 2018	IGSAB	13/02/2018
v2.0	Information Governance Manager	Minor amendments	May 2018	IGSAB	13/02/2018 (further subsequent minor amendments authorised)