UNIVERSITY OF PORTSMOUTH

INFORMATION GOVERNANCE POLICY

August 2020

Contents

Summary 4
What is this document about? 4
Who is this for? 4
Who can you contact if you have any queries about this document? 4
Executive summary 4
Statement of Strategic Intent 5
1. Why have a strategy for Information Governance? 6
2. How will the strategy be implemented? 8
3. Principles 9
4. Accountabilities and Responsibilities 10
Appendix 1 13
Information Governance 13
Information 13
Records 13
Records Management 13
Documents 14
Declaration 14
Personal Data 14
Processing of Information 14
Classification of Information 15
Appendix 2 17
Appendix 3 18
Legislation 18
Audit & Regulatory Requirements 18

Document title		
Information Governance Policy		
Document author and department		
Sarah Arnold, University Records Manager & Samantha Hill, Information Disclosure and Complaints Manager		
Approving body		
Information Governance Group		
Date of approval		
August 2020		
Review date		
July 2023		
Edition no.		
2		
ID Code		
223		
Date of effect		
September 2020		
EITHER For public access online (internet)? *Tick as appropriate*		**YES**
OR For staff access only (intranet)? *Tick as appropriate*		
For public access on request copy to be mailed *Tick as appropriate*		**YES**
Password protected *Tick as appropriate*	**NO**	
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk If you need this document in an alternative format, please email corporate.communications@port.ac.uk		

The latest version of this document is always to be found at:

http://policies.docstore.port.ac.uk/policy-223.pdf

Summary

What is this document about?

This policy concerns the governance of information processed by the University of Portsmouth (hereinafter referred to as the University).

Who is this for?

This policy is aimed at all individuals responsible for the processing of University information.

Who can you contact if you have any queries about this document?

Any questions about this policy should be directed to Samantha Hill and Sarah Arnold via information-matters@port.ac.uk

Executive summary

Without good governance of information:

- the University would be unable to function effectively and any decisions made regarding the future strategic direction of the University would be fundamentally flawed; and,
- the University would not be able to comply with its legal and regulatory obligations, leading to financial penalties and reputational damage.

Therefore, the University recognises that information is a corporate asset, the correct management of which is vital to support the University's core functions and wider strategic aims. This policy formalises the University's commitment to Information Governance and, together with its' accompanying action plan, risk assessment and communications plan, will aim to create an effective, consistent and holistic approach to the governance of information across the University. The aim is to facilitate teaching, research, business functions and the University's other strategic objectives.

All staff, at all levels in the University have a role to play in the successful implementation of this policy. The policy sets out those roles and responsibilities, as well as a commitment from the University to ensure all staff have the appropriate induction, training and supervision to carry out their roles effectively.

Statement of Strategic Intent

The University recognises that information is a corporate asset, the correct management of which is vital to support the University's core functions and wider strategic aims. For the University to manage its information effectively and pro-actively, there must be an understanding of the University's information needs, how these can be met and how that in turn underpins the University's strategic objectives.

The University is committed to:

- governing its information in compliance with the requirements of the legal and regulatory framework within which it operates;
- creating and maintaining a positive Information Governance culture within the University;
- ensuring that all University staff are aware of their responsibilities with regard to Information Governance, are trained to carry them out and have sufficient resource, knowledge, skills and expertise so to do;
- adhering to the information principles (set out in Section 3);
- adopting best practice in Information Governance and developing information management systems which support and assist this; and,
- attaining appropriate ISO standards, data seals and other relevant accreditations associated with Information Governance;

The majority of future information will be created, managed and preserved digitally. However much historic information is still paper-based. This policy applies to all information regardless of medium, although priority should be given to developing digital solutions and enablers.

Four common themes run throughout this policy:

Legal compliance
Security
Flexible working
Quality and consistency

---

1. Why have a policy for Information Governance?

Without good governance of information:

- the University would be unable to function effectively and any decisions made regarding the future strategic direction of the University would be fundamentally flawed; and,
- the University would not be able to comply with its legal and regulatory obligations, leading to financial penalties and reputational damage.

In addition, the University has a duty of care to manage the information it processes correctly. It is the right thing to do. This policy is required to demonstrate that the University formally recognises information as a valued asset and is committed to continual improvement with regard to the way in which it processes that information. This policy applies to all University information (paper and electronic) and all information systems of work (manual process or electronic/automated systems) put in place to process University information.

The key terms used in this policy and other Information Governance policies are defined in Appendix 1.

1.1. Aims of the Policy

This policy has three core aims:

The first aim of this policy is to underpin the University's Strategy 2025 and the University Vision 2030 through an effective, consistent and holistic approach to the governance of information across the University, in order to facilitate teaching, research, business functions and the University's other strategic objectives. Specific examples can be found in Appendix 2.

The second aim of this policy is to ensure that information is valued as an asset and is proactively managed as such. Staff will have the skills to manage information effectively so that the University can evidence the importance of a single source of information.

The third aim of this policy is to realise the benefits of effective information governance, including:

- Operational efficiency – cost, time, space.
- Compliance with regulatory and legal obligations – Freedom of Information (FOI), General Data Protection Regulation (GDPR) and Records Management.
- Accountability and reduced risk.

1.2. Background

1.2.1. Legal, Audit and Regulatory Context

The University operates within a legal, audit and regulatory framework, which governs how we process our information (see Appendix 3 for further details). A breach of the GDPR can lead to fines of up to 20 million Euros. However, poor Information Governance practices may also contribute to fines under other legislation (e.g. Health & Safety legislation requires the University to create and maintain certain records and failure to do so may result in fines, or mean that the University is unable to defend itself against claims of compensation following an accident). In all cases, the cost of the fine would be minimal compared with the reputational damage to the University, and the financial cost of rectifying any breach and preventing recurrence.

1.2.1.1. Strategic Implications

- The legal, audit and regulatory framework in which the University operates does not change at the same pace as technology, which can lead to conflicts between the desire to make use of the latest technological developments and the need to demonstrate compliance.
- Future technical systems used for the management of information must enable the University to comply with the requirements of the legal, audit and regulatory framework within which it operates.
- The University must preserve information required for legal, audit and regulatory reasons. This presents challenges where that information resides in obsolete databases.
- The University needs to be open and transparent in all its dealings, as information may need to be disclosed.

1.2.2. Principles of Information Governance

In order to ensure the effectiveness of this policy, the University will need to adhere to certain principles of Information Governance. These are:

We can rely on the authenticity of information.
We are sure of the reliability of information.
We can rely on the integrity of information.
We are able to find, access, read and use the information.

Further explanation of these principles can be found in Section 3.

1.2.3. Information Risk

In order to prioritise work and resources, the University needs to have an understanding of the current and potential risks associated with Information Governance. This policy will be accompanied by a risk register, which will be periodically updated. It will identify and prioritise the current risks to the University from an Information Governance perspective. These will include:

- Legal and regulatory risk
- Security risks
- System design risks (technology or process based systems)
- Cultural risks

1.2.4. Information Culture

The information culture describes the way in which Information Governance is perceived, valued and embedded across all levels of an organisation. An empowered and effective implementation of this strategy should result in a positive and proactive information culture, indicators of which include:

- Effective induction, training & awareness raising.
- Staff value the information with which they work.
- Staff understand the importance of managing information correctly and consistently.
- Poor practice is challenged.
- Managers lead by example.

- Staff feel confident to ask questions and safe to raise concerns.
- Information Governance is considered when designing new systems and processes, or as a key part of any new project.

2. How will the policy be implemented?

In order to implement the statement of strategic intent and achieve the aims of this policy, actions and enforcement will be required.

2.1. Information processing rules

Information must be managed holistically and consistently, in accordance with rules defined by the University. This policy will be accompanied by an agreed, SMART action plan (Specific, Measurable, Achievable, Relevant and Time-bound), which will determine the rules that are required to enact this policy and address the risks identified by the University in relation to Information Governance, including but not limited to:

- Defining where and how information should be stored.
- Creating a framework governing the effective processing of information, which is consistent, conforms to accepted standards, and which will (in the longer term) reduce the effort required to process the University's information.
- Enhancing a programme of continual improvement around the accuracy, reliability and completeness of information, focusing on the single source of information.
- Reducing unnecessary duplication of information and its storage.
- Ensuring that information no longer required by the University is reviewed, disposed of confidentially, transferred, anonymised, or archived in a timely manner.
- Reviewing and updating, if appropriate, all current policies, procedures, training courses and guidance materials related to Information Governance.
- Development of any additional training and guidance materials necessary to enact this strategy.
- Development of a communications plan associated with this strategy.
- Actively designing Information Governance in to processes and systems at the outset.

Completion of the action plan will be overseen by the Information Governance group and, once completed, the University will undertake to proactively enforce and periodically review the processing rules.

2.2. Information Users

Information is a corporate asset – it belongs to the University but is managed and maintained by staff through defined accountabilities and responsibilities. These are outlined in Section 4. The University will undertake to enforce these accountabilities and responsibilities via appropriate supervision, line management and appraisal/development processes.

2.3. Training for Information Governance

As a minimum, the following training is provided for University staff:

- All staff will read the Information Governance policies as part of their formal induction into the University.
- All staff will undertake the Information Governance eLearning package every 2 years. A link to the eLearning package can be found on the Information Matters staff page.

- Staff with specific Information Governance responsibilities within their area may take part in the Information Governance Champions training events.
- Ad-hoc training will be provided by the Information Governance team on request.
- Training on the use of specific corporate systems is provided by the University (e.g. training on the Student Records system is provided by IT Training) and will support Information Governance good practice.

Training will be developed and enhanced to support the implementation of this policy. Where the training is not provided by the Information Governance team, agreement will be reached with the providing department on the best way to achieve Information Governance requirements.

In addition, current guidance materials on Information Governance will also be updated and enhanced to support the implementation of this policy.

2.4. Communicating the Policy

The action plan for this policy will be accompanied by a communications plan, which will also be overseen by the Information Governance group. The communications plan will be engaging and inform those, at whom this strategy is aimed, of the following:

- the processing rules created under this policy;
- their accountabilities and responsibilities under this policy;
- the training available to them;
- the pre-existing guidance and support available to them in relation to Information Governance; and,
- the consequences of non-adherence to the policy.

The Information Governance team will also use a network of Information Governance Champions to assist with the communication and implementation of this policy across all business areas.

3. Principles

3.1. We can rely on the AUTHENTICITY of information

An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; and created or sent at the time purported. (ISO 15489 Records Management)

- Information is created and maintained in the best format for the purpose.
- The University has the relevant information needed to form a reconstruction of activities or transactions that have taken place to ensure the continued operation of the University.
- Information can be proven to be what it claims to be through version control and adherence to guidelines.
- Holders of master records are identified to ensure that information is not duplicated unnecessarily throughout the University.

3.2. We are sure of the RELIABILITY of information

A record is considered reliable if its contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. (ISO 15489 Records Management)

- The regulatory and legislative requirements for the management of information are met.
- Ownership and responsibility for managing University information is clearly established.
- The University will know what information it holds and where it is held.
- Historical accountabilities are met and information of long term value is identified and preserved as archives.
- Information Governance supports resilience of business processes and business continuity.
- Information is appropriately destroyed when no longer required.

3.3. We can rely on the INTEGRITY of information

Records will have integrity if they are complete, unaltered and protected from unauthorised alterations. (ISO 15489 Records Management)

- Information provides adequate evidence of the business activity to which it relates.
- Information complies with the record keeping requirements of best practice outlined in relevant standards and legislation.
- Information required by staff, students and members of the public is provided in a timely and cost effective way.
- Information is protected against unauthorised access, alteration, deletion or disclosure.

3.4. We are able to USE the information

A usable record is one that can be located, retrieved, presented and interpreted. The links between records that document a sequence of activities should be maintained. (ISO 15489 Records Management)

- Systems to be fit-for-purpose and effective.
- Users to understand why information must be managed effectively.
- Users to have skills they need to manage information, supported by relevant training.
- Information is available and easily accessible at all times to authorised users as required.
- Inconsistencies and errors in storage and access to information minimised.
- The qualities of accessibility and interpretation are maintained for as long as the record is required.

4. Accountabilities and Responsibilities

4.1. All Staff will:

- understand their responsibilities and accountabilities with regard to Information Governance and / or know who to approach for advice and guidance;
- be responsible for effectively managing information in their own areas, in accordance with University policies and any legal/regulatory requirements specific to their areas;
- maintain confidentiality;
- be aware of the best place to store information;
- understand what needs to be preserved as a record and what does not;
- declare documents as records when appropriate (a definition of “declaration” can be found in Appendix 1); and,
- report any data breaches immediately.

Staff must not, by their actions or omissions, undermine the University's compliance with its legal and regulatory framework. Failure to follow the University's policies or procedures may result in disciplinary action.

4.2. Line Managers and Supervisors will:

In addition to the requirements on All Staff:

- ensure that all new staff receive a full induction;
- monitor their team's compliance with Information Governance policies, procedures and good practice;
- identify training needs with regard to Information Governance;
- co-operate with the Information Governance team and local Information Governance Champions; and,
- promote a positive and proactive Information Governance culture within their teams.

4.3. The Information Governance Team will:

- provide advice, guidance and training to all staff at all levels on Information Governance;
- create and maintain policies and procedures relating to Information Governance;
- identify information risks to the University and recommend action to reduce the impact and/or likelihood of that risk;
- promote a positive and proactive Information Governance culture across the University; and,
- raise awareness of Information Governance good practice across the University.

4.4. Information Governance Champions will:

- promote a positive and proactive Information Governance culture within their section of the University;
- act as a conduit between business areas and the Information Governance team;
- challenge poor Information Governance practice; and,
- escalate risks, issues or concerns to the Information Governance team.

4.5. The Information Governance Group will:

- be responsible for overseeing, maintaining and reviewing this policy;
- define and endorse the action plan associated with this policy;
- define and endorse the risk register associated with this policy;
- provide a forum for collaboration on matters of information governance;
- have oversight of all IG related projects / activities across the University;
- co-ordinate the Information Governance message; and,
- escalate risks or issues arising to UEB, where appropriate, via the Executive Director of Corporate Governance.

4.6. Senior Management will:

- commit to the deliverance of this policy;

- provide proactive leadership in respect to Information Governance and demonstrate commitment to this policy;
- create and foster a positive and proactive University culture with regard to Information Governance; and,
- ensure adequate resources are available.

4.7. Staff involved in the procurement, implementation, maintenance, development and decommissioning of corporate systems will:

- ensure privacy by design;
- consult with the Information Governance team, as appropriate, before commencement of, and during, the project;
- co-operate with the Information Governance team; and,
- ensure any data processors are aware of their obligations under GDPR.

4.8. Data Owners will:

- Approve data glossaries and other data definitions;
- Ensure the accuracy of information as used across the Enterprise;
- Direct Data Quality activities;
- Review and pprove Master Data Management approach, outcomes, and activities;
- Work with other Data Owners to resolve data issues and dissonance across business units;
- Second level review for issues identified by Data Stewards; and,
- Provide input to the IT Governance Board on software solutions, policies or Regulatory Requirements that impact their data domain.

4.9. Data Stewards will:

- Serve as a subject matter expert (SME) for their data domain;
- Identify and work with other data stewards to resolve data issues;
- Improve data quality in their data domain;
- Champion data improvement activities in their data domain, e.g. creation of data dictionaries, data standards, etc.;
- Act as a member of the Data Stewards Working Group;
- Propose, discuss, and vote on data policies and committee activities;
- Report activities and decision of the Stewards to the Data Owner and the other Stakeholders within a data domain;
- Ensure that Stakeholders' interests are represented at the Steward's Council; and,
- Work cross functionally across lines of business to ensure their domain's data is managed and understood.

Appendix 1

Definitions used in this policy

Information Governance

Information Governance is a framework of policies, procedures and controls to manage information in a joined-up way. It involves knowing:

- What information is held.
- Where it is held.
- Who is responsible for it.
- How long to keep it.

Information Governance also involves establishing effective procedures for all aspects of information processing, including creation, maintenance, storage, use, retention and destruction.

Information

University Information can be divided into two broad categories: Records and Documents.

Records

A Record is information produced or received as a result of a business activity and retained as evidence of that activity. It may be in any format (e.g. paper, fax, drawing, plan, video, slide, microfilm, audio recording, CD, email, social media posts, tweets etc). Records can be subdivided into three sub-categories:

Structured Records

Records held as data in a structured, relational database.

Semi-structured Records

Records wherein the layout, composition and content are constrained by the use of approved templates (e.g. forms), to such a degree that a computer could be scripted to identify specific content blocks and take action based upon them (e.g. OCR/ICR, metadata extraction, process automation).

Unstructured Records

Records where the layout, composition and content are at the discretion of the author.

Records have a finite retention period, as set out in the University Retention Schedule. This retention period applies regardless of format. Records which have a historical value which outlasts their retention period should be transferred to the University Archive. This is also stipulated in the University Retention Schedule.

Records Management

This is the “corporate function responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records” (ISO 15489 Records Management).

Documents

Documents themselves have no long term value and the University has no requirement to create or preserve them. They are created to assist in the day-to-day duties of an individual or team and are managed at the discretion of the individual or the team. However, it should be noted that documents containing personal data are still subject to data protection legislation (GDPR) and documents may still need to be disclosed under various legislative acts. Therefore, some degree of management and University oversight is still required for documents. This is known as Document Management.

Declaration

Documents may become records, for example, when a draft policy is ready to be sent out for formal submission, because from this point onwards it is important to the integrity and authenticity of the final policy that the draft text that went forward for approval is recorded. This process is known as Declaration and involves the transfer of the document into an official records management system (be that paper or electronic), followed by the deletion of the document from its previous location(s), and the application of the University Retention Schedule.

Personal Data

Personal data is any information, including facts and opinions, that identifies a living individual. Personal data can be found in both records and documents.

Special Categories of Personal Data

Special categories of personal data relate to issues of:

- race or ethnic origin of the data subject;
- political opinions;
- religious beliefs or beliefs of a similar nature or no belief;
- trade union membership;
- physical and/or mental health;
- sexual life or sexual orientation;
- genetic and biometric data; and,
- Commission of criminal offences or alleged criminal offences.

Data Subject

The individual who is identified by the personal data collected.

Processing of Information

Processing is the collective term for any action taken relating to personal data, including:

- obtaining;
- creating;
- recording;
- storing;
- using;
- disclosing;

- sharing;
- destroying;
- anonymising/pseudonymising; and,
- rectifying, amending and updating, where appropriate.

However, in this policy, the same term also relates to these same actions for non-personal information.

Data Controller

The organisation that determines the need to collect personal data and the uses to which it will be put. All Departments, Schools and sections of the University, form part of the legal entity which is the University, which is a data controller.

Data Processor

A third party which processes personal data on behalf of the University.

Classification of Information

If read by unauthorised persons, lost or damaged then some information has the potential to:

- harm academic relations;
- breach copyright;
- cause considerable departmental embarrassment;
- cause considerable inconvenience to staff or students;
- damage operational effectiveness or security;
- cause considerable financial loss;
- facilitate fraud, improper gain or advantage for individuals or third parties;
- jeopardise an investigation;
- facilitate the commission of crime; or,
- undermine the proper management of a Department/School/Service.

By understanding the impact potential and classifying the information on that basis, we can suggest the most effective ways to process this information – in terms of backup, encryption, rules for safe transmission and disposal etc. Classifying information enables us to focus resources on its protection more effectively.

The confidentiality of information may reduce over time, so access restrictions should be subject to regular review. Restricted information may still need to be disclosed after appropriate consideration by the Information Disclosure team and, if necessary, redaction. Staff are expected to act responsibly with regard to any information they have access to as part of their role.

Non-Confidential Information

In order to facilitate collaboration and sharing of documentation between departments an open and transparent approach is being taken to University information. Unless information meets one of the restricted criteria below, the University will not actively prevent all staff having access to it.

Restricted Information

There are three types of information which we classify as RESTRICTED:

- Personal data (see definition above), including special categories.
- Commercially sensitive data:

- Financial, commercial, scientific or technical or other information the unauthorised disclosure of which could reasonably be expected to result in a material financial loss to the person or organisation to which the information relates, or could prejudice the competitive position of that person in the conduct of his or her profession or business or otherwise in his or her occupation.
- Information the disclosure of which could prejudice the conduct or outcome of contractual or other negotiations of the person to whom the information relates.

- Intellectual property.

Transfer of Restricted Information

Any transfer of restricted information to a third party must be carried out securely. As a minimum, paper records should be sent by a trusted courier service. Best practice should be that the paper records are delivered by hand by the officer responsible for the transfer (where feasible), directly into the hands of the officer in the third party to whom responsibility for the information has been assigned.

Electronic records should, as a minimum, be encrypted and either sent over a secure connection or put onto a CD and delivered by a trusted courier service. Best practice should be that the records are encrypted and the password provided separately by another means. Again, electronic records on an encrypted CD should preferably be delivered directly by the officer responsible for the transfer (where feasible), directly into the hands of the officer in the third party to whom responsibility for the information has been assigned.

Any queries about restricted information should be directed to information-matters@port.ac.uk.

Appendix 2

Specific examples of Information Governance underpinning the University's Strategy 2025 and Vision 2030

The members of the Information Governance team will be working with colleagues in many ways towards the specific elements of the University Strategy and Vision, including the following;

- Transforming Alumni relations and advancement activity – ensuring that our privacy notices and data processing practices allow us to contact our alumni legally and in a transparent way, which will give our alumni confidence that they are dealing with an open and trustworthy organisation.
- Lead in environmental sustainability and become climate positive by 2030 – by ensuring that we are keeping only the information we need, only for as long as we need it, as well as eliminating unnecessary duplication, thereby reducing the carbon footprint of our information processing storage both paper and electronic. This can also lead to enhancing the University's estate by reducing the need for space for holding paper based records.
- Significantly building our Global reach and reputation – by ensuring we comply with record keeping requirements of all international countries with which the University has business; ensuring we have data sharing agreements in place where necessary, and complying with the registration requirements of the ICO for our overseas offices.
- Engaging every student in a life-changing experience – by ensuring that all information provided to students by the University is accurate, consistent and up-to-date, and that their lifelong record is always available to them by building information curation into new systems and processes.
- Delivering globally-recognised research and innovative solutions that improve society - assisting researchers with their data management plans and data privacy notices so that their research is conducted on a firm foundation.

Appendix 3

The legal, audit and regulatory framework

The University operates within a legal, audit and regulatory framework, which governs how we process our information. This includes, but is not limited to:

Legislation

- General Data Protection Regulation (GDPR) and the Data Protection Act 2018
- Limitations Act 1980
- Freedom of Information Act 2000
- Environment Regulations 2004
- Equality Act 2010
- Employment Act 2002
- Health & Safety at Work Act 1974 (and associated regulations)
- Human Rights Act 1998
- Value Added Tax (VAT) Act 1994
- Companies Act 2006

Audit & Regulatory Requirements

- Office for Students (OfS) requirements
- United Kingdom Visas & Immigration (UKVI) requirements
- National reporting requirements, e.g. Higher Education Statistics Agency (HESA)
- Audit requirements, e.g. Quality Assurance Agency for Higher Education (QAA)
- Transcript & Validation provision
- Research and Teaching Excellence Frameworks (REF/TEF) submissions
- Consumer Marketing Agency (CMA) requirements
- Funding Council requirements
- Professional Accreditation requirements
- Safeguarding & Prevent requirements
- ISO and British standards

University of Portsmouth
Corporate Governance
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3195
F:
E: corporate-governance@port.ac.uk
W: www.port.ac.uk