Document Management Policy
IGP-05

Summary			
This Policy establishes standards for document management across all of the University's functions and operations, and for ensuring documents are created, maintained and disposed of appropriately, taking full account of operational needs.			
Scope			
This policy applies to all members of the University and any individual creating or handling documents on the University's behalf.			
Document Control			
Document type	Information Governance Policy – IGP-05		
Document owner	Information Governance Manager		
Division	University Secretary's Office		
Lead contact	Information Governance Manager		
Document status	Approved		
Version	v1.2		
Approved by	Information Governance and Security Advisory Board & University IT Committee	Date	19/04/2018
Date of publication	July 2018	Next review date	
Date of original publication	July 2018	Revision frequency	
Superseded documents	N/A		
Related documents	See **13. Interaction with other legislation and policies** below		

Contents

1. Introduction

Documents are a vital part in the effective functioning of any organisation. We need documents on a short-term basis to help us to work consistently and productively and to keep track of progress in projects and activities. Creating standards for document management and ensuring that documents are created, managed and disposed of appropriately is a key part of good information management that will improve efficiency and mitigate legal and compliance risks (e.g. requirements relating to data protection, tax and employment). This must also be supported with the necessary guidance and training for staff to ensure they are confident document handlers.

2. Purpose of this Policy

The University must ensure that documents created in relation to its operations are being managed and maintained appropriately. This policy sets out standards and definitions to enable staff to create documents that:

- Meet the University's internal requirements
- Enable the content of the document to be accessed, used and reused in a controlled and efficient manner
- Ensure the continuity of University operations in the event of staff absence or emergency circumstances
- Are compliant with all regulatory and statutory requirements
- Enable the defence of the rights and interests of the University and its stakeholders

- Are capable of providing evidence of a decision or operational process
- Are kept and maintained and stored in the most economical way consistent with the above objectives

3. Scope

This policy applies to all members of the University and any individual creating or handling documents on the University's behalf.

The policy applies to all documents held in any format, 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 (other than voicemail messages)

Voicemail, text or instant messages do not constitute documents for the purposes of this policy, unless recorded or retained for specified purposes in accordance with legal requirements.

Specific guidance in relation to the processing and storage of research data can be provided by the Research Data Service and the Research Data Storage Facility (RDSF) can be used for storing research data.

4. Definition

ISO9000 defines a document as "*information and its supporting medium"*, meaning that it can include a wide range of both hard copy and digital formats and is not simply limited to written information. It can also be a photograph, video or audio record of an event.

5. Roles and responsibilities

The **Senior Information Risk Owner (SIRO)** is accountable at an executive level for ensuring that the University has robust information governance and security processes and procedures in place – this includes document management. 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. This policy sits under the wider Information Governance Framework.

Information Asset Owners (IAOs) are responsible for ensuring that any information assets they own are managed in accordance with this policy, and also for maintaining standards in

relation to document management in their operational area. Information asset owners are listed in the University's information asset register.

Information Asset Administrators (IAAs) are members of staff that have been delegated responsibility by an IAO for the operational use of particular information assets.

The **Information Governance Manager** has operational responsibility for this policy and ensuring that it complies with legal and regulatory requirements. They are also responsible for providing learning and development materials relating to key points from this policy and for monitoring its overall effectiveness.

All staff are responsible for creating and using documents in line with the terms of this policy.

6. Document lifecycle

All documents created have a "lifecycle" from creation through to disposition, as shown below:

It is important to understand this cycle and the various stages when creating and handling documents to ensure that they are managed effectively.

1.1 Creation

Documents that will represent formal, compliant and trusted communications or records must be well-designed from the point of creation, using relevant naming conventions and document templates when necessary. All staff must act responsibly, lawfully and professionally when creating documents relating to the University's activities and/or on the University's systems.

1.2 Distribution

When documents are transmitted or otherwise made available to those who need them and, upon receipt, are used in the conduct of the University's operations.

1.3 Use

Use takes place after a document has been distributed internally, and can generate business decisions, further actions, or serve other purposes.

1.4 Maintenance

While a document is in active use, it is vital that the content is maintained, accurate and available to those who require it at all times.

1.5 Disposition

The practice of handling information that is accessed less frequently or has reached its assigned retention periods. This could mean destruction of the document(s) or transfer to an archive until the assigned retention period is reached. The University's Records

retention Schedule (IGP-04) sets out retention periods for various categories of information.

7. Document management practices

The below list sets out practices that must be adhered to when creating and handling documents on behalf of the University:

- Documents must be clearly named (with date and version number if relevant) and stored in a structured manner (see section 8)
- Duplicate copies of documents must not be created unnecessarily
- Wherever possible, documents must be shared from their source location rather than attaching documents to emails
- Key documents (that others may require access to) must be stored in an appropriate shared filestore, i.e. not personal filestores (including desktop or device filestores)
- Copies of documents, whether digital or hard copy, must only be taken offsite when necessary (encrypted and password-protected removable storage or remote access via a secure network connection must be used whenever possible)
- Digital copies of document should never be emailed to a personal email account or stored on a personal cloud-based storage account
- Once a document is finalised, previous versions and drafts of documents should only be retained where entirely necessary e.g. for legal or audit purposes
- Appropriate metadata (such as title and tags) should be included at the point a new document is created to ensure it can be easily located and retrieved
- Any metadata contained in documents that have been created from previous versions or from templates created by another person should be deleted and/or updated
- Final copies of formal documents (such as policies or minutes) must be saved in PDF format
- As standard practice, the filename and storage location should be included in the footer of the document
- Formal documents that will be used and edited in the long term must include a document history or version control box to allow users to see the development of the document over time
- Regular audits (at least annual) of digital and hard copy information must be conducted to ensure that information is not retained longer than it is required (see Records Retention Schedule for retention periods)

8. Naming conventions and folder structures

A naming convention is a collection of consistent rules followed in naming documents, which should allow users to work effectively, ensure that files can be easily accessed by all who require access and to ensure that individuals are referring to and working on the correct document. The use of consistent naming conventions will improve efficiency by allowing staff to quickly identify the nature of the information contained within a document when searching through an archive or filestore. For further information, please see relevant guidance on naming conventions.

Folder structures and names are also important in allowing the efficient retrieval of documents. The below principles must be followed when creating new folder structures:

- Folders must be clearly named by a relevant and meaningful subject area
- The names of individuals should only be used when creating a case file, i.e. not creating a personal folder in a shared filestore
- Top level folders must be kept to a minimum
- Ideally, file structures should not exceed six levels of subfolders
- Appropriate access levels must be assigned depending on necessity to access the documents contained within the folder

9. Information Classification Scheme

The University has an information classification scheme, including five levels of security classification for different types of information, as below:

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Open	Available to all authenticated members of University staff
Confidential	Available only to authorised and authenticated members of staff
Confidential & Sensitive	Access is controlled and restricted to a small number of named, authenticated members of staff
Secret	Known only to a very small number of authenticated members of staff

While it is not mandated that all documents and records are marked with the relevant classification, it is good practice to include the classification in the document header or footer, or by way of a watermark (on a digital copy) or stamp (on a hard copy), to ensure that users and recipients are aware of the potential sensitivity of the content.

Staff should consider the following questions and exercise their judgement in each case:

Does the document contain information that originated from an open and publicly-accessible source?	Provided the document contains information that was not obtained in breach of any confidentiality or secrecy obligation and is in the public domain, the document may be classified as open or public depending on the other questions to be considered below.
Does the document contain personal data?	See the Data Protection Policy for a definition of “personal data”, but as a general guide this is any information that may directly or indirectly identify an individual (called a “data subject”). Documents that contain personal data should be classified as Confidential.
Does the document contain special categories of personal data or personal data	See the Data Protection Policy for a definition of these categories of personal

relating to criminal convictions and offences?	data. This information requires additional procedures to be followed and safeguards applied and should be classified as Strictly Confidential.
Does the document contain any information of commercial or competitive value for the University or any other third party?	The document may contain commercially sensitive information or trade secrets relating to the University or entrusted to the University by a third party or information relating to the University's strategic plans and market opportunities.
If the document was accidentally disclosed, would it pose a risk to any individual(s) or the University?	The document may contain information which would have an adverse impact on one or more individuals or groups within the University, the University as a whole (including reputational harm) or the University's agents, suppliers or other partners.

10. Digital preservation

Where documents or records are either "born digital" or where hard copies are digitised, the University will ensure that there are appropriate standards and guidance in place to ensure that records of permanent or continuing value remain accessible and preserve their integrity for as long as required, accounting for changes in IT software and hardware.

Adherence to these standards and guidance will safeguard the authenticity and integrity of digital materials in the long term and will allow the storage of digital materials safely through adoption of security mechanisms appropriate to each classification of material.

11. Destruction

All documents must be subject to action proscribed in the University's Records Retention Schedule (IGP-04), which may be destruction, at the end of the assigned retention period unless such period has been suspended on learning of an actual or reasonably anticipated claim, audit, investigation, subpoena or litigation asserted or filed by or against the University.

IAOs and IAAs should periodically determine whether any documents under their control should be destroyed in accordance with the Records Retention Schedule.

12. Education and training

Relevant training and education materials will be provided to ensure that staff are aware of their responsibilities in relation to document management.

13. Interaction with other legislation and policies

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

- IGP-01 - Information Governance Policy
- IGP-02 - Data Protection Policy
- IGP-03 - Records Management and Retention Policy
- IGP-04 - Records Retention Schedule
- IGP-06 - Digital Preservation Policy
- IGP-09 - Information Strategy Principles
- IGP-10 - Information Classification Scheme
- Information Security Policy
- IT Acceptable Use Policy
- Information Handling Policy
- Guidance on the Retention of Research Records and Data

All documents processed on behalf of the University must comply with the various legislation relevant to information governance and security.

14. Policy review and ownership

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

Document history					
Version	**Author / Primary reviewer**	**Details of changes**	**Date**	**Approved by**	**Approved date**
d0.1 Draft	Information Governance Manager	Initial draft – new policy	Aug 2016	N/a	
d0.2 Draft	Information Governance Manager	Minor changes	Nov 2016	IGSAB	17/11/2016
v1.0 Approved	Information Governance Manager	Minor changes required by IGSAB	Nov 2016	University IT Committee	17/05/2017
v1.1 Approved	Information Governance Manager	Review by external legal advisor	Feb 2018		
v1.2 Approved	Information Governance Manager	Incorporated changes by external legal advisor and sanitised against other policies	July 2018	IGSAB	19/04/2018