Introduction
The University creates, receives and holds information in a range of formats. All information must be managed appropriately in relation to its content, purpose and ongoing value.

This guidance note is designed to help staff identify the key issues they should consider in relation to managing information and to direct them to other relevant information or resources where appropriate. It is not intended to provide all-encompassing procedures/protocols but rather to provide an overview of good practice for staff. Further information can be found in the corresponding guidance notes which are available on the Records Management section of the website www.strath.ac.uk/foi/recordsmanagement.

Why do we have to manage information and records?
By managing information appropriately the University will ensure that it can work in a more efficient manner, as staff will be able to create, locate, understand, and retrieve information as and when required.

Good information and records management involves:

- having an organised approach to record-keeping
- sharing information appropriately
- being able to locate and retrieve records when required
- providing evidence of activities, decisions and actions
- ensuring adherence to relevant legislation including ‘access to information’ regimes (see Legislative requirements)
- keeping what you need only for as long as is required (depending on administrative, legal or statutory requirements).
- ensuring long-term preservation of records of archival value to maintain the corporate memory.

Following best practice in relation to information and records management should ensure (among other things) that:

- administration of the University is more efficient as information is easier to find, is reliable, and is secure.
- the University spends less time and money managing information that is not required.
- the risk of a security breach/breach of the Data Protection Act is reduced as appropriate security is applied to information.
- the University can evidence its activities, decisions and actions with robust and reliable records.
- the University is able to comply with external requirements e.g. audit/funding requirements.
- the University is compliant with the Code of Practice on Records Management under S61 of the Freedom of Information (Scotland) Act. This provides a best practice framework which organisations are expected to take into consideration.

RM Guidance Note: 10 Managing Information and Records Top Ten Key Points
What do we need to manage and why?
The University recognises that not all information is of the same value. Some information is ephemeral and will not have to be retained for any period of time. Other information will constitute a ‘record’ and will have to be retained to provide evidence of activities, decisions and actions taken by the University. It is also important to identify records of archival value which require to be preserved permanently by transferring them to the University’s Archives. This will ensure that the ‘corporate memory’ is maintained.

What is a record?
A record is a document, regardless of format or medium (it could be paper or electronic) which is held by the organisation (whether it created or received it) and which:
- records the transaction of a business process,
- provides evidence of a business activity,
- is a historical record which is required for the corporate memory,
- is required for legal or statutory compliance.

The University creates, receives and holds records relating to all of its functions, whether administrative or academic. ‘Records’ are valuable to the organisation and as such these require to be managed from the point of creation through to ultimate disposal/destruction.

Who is responsible for records?
All staff who create, receive, and use records in the course of their job are responsible for ensuring records are managed appropriately. It is therefore likely that the majority of University staff will have some responsibilities in relation to record-keeping as part of their job.

Heads of Departments within the University have overall responsibility for the management of records generated by the activities within their departments.

See the University’s Records Management policy for more information.

Creating Records
These days much information is created and held in a digital format. However, a great deal of information is still produced and held in hard copy. No matter what the format, we should manage our records appropriately and this involves considering the first step in a record’s ‘lifecycle’: its creation.

Some records are created automatically for you. At other times, you must make a conscious decision to create a record. Records should be created where they are needed to support business activities or to provide information or evidence about activities, transactions or decisions.

Deciding what records to create should be based on:
- business needs
- relevant regulatory or legislative requirements
- internal and external accountability expectations
• assessing the potential risks that may arise from failing to capture adequate records.

Key points to remember:

• Records may be created in any format, including paper, electronic or digital media, as long as their usability, reliability and integrity can be preserved for as long as the record is needed.

• Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why.

• Records should be created at the time of, or as soon as practicable after, the event or transaction to which they relate to ensure they are accurate and reliable.

• Duplicate records or multiple copies of the same record should be kept to a minimum. There is normally only a need to retain one ‘master’ copy of each record – this will help to ensure the integrity and reliability of records.

• ‘Convenience copies’ may be required by individuals for a short period of time i.e. copy of papers/agendas when attending a meeting. However, these should be destroyed as soon as they are no longer required.

RM Guidance Note: 1 Creating Records

Naming Records
For records to be of use and value to the University we must be able to locate and retrieve them when required. For this to happen records must be stored in the most appropriate location and must be easily identifiable. All records – whether paper or electronic – must be organised logically, so that they can be easily and speedily retrieved.

Good titles and names are essential so that information can be promptly identified and retrieved. All records, whether paper or electronic, should (in most cases) be named so that their contents can be easily identified without opening the document/file.

To make naming records easier within your team you should consider:

• how you name your records and agree a format within your team. This will make it easier to identify and retrieve documents in the future without having to open each one to see the contents.

• using version control for documents. This will make it easier to follow the progression and development of a document. It will also make it easier for you and others to identify the most recent version.

RM Guidance Note: 2 Naming Records
RM Guidance Note: 3 Version Control
Filing Records
At the point of creation records should be given a meaningful name which will aid users identify the content of the record. Records should then be filed into an appropriate location. All team members who have responsibility for filing records should be aware of the appropriate location to file them to.

Key Points to Consider:
- the information you handle on behalf of the University belongs to the University.
- have an agreed procedure within your team as to where certain types of records are filed/stored. This may be a hard copy or digital filing system. Ensure all staff are aware of this procedure.
- where possible and appropriate records should be stored in a shared storage facility where team members can access ‘team records’. This is likely to be on a shared drive/system located on a University server.
- do not create information siloes by storing information where it is inaccessible to others who require access to it i.e. on your C drive/personal H drive.
- do not store records on your desktop/C drive – these are not backed up on the University’s servers. If your computer/laptop is damaged these will be more difficult (and in some cases) impossible to retrieve.
- If information is ‘confidential’ or contains personal data and therefore needs to restricted in terms of access then ensure that you are filing it to a location which is suitably secure. The IT Helpdesk can assist you with restricting permissions on folders on a shared drive.

RM Guidance Note: 4 Filing Records

Email Management
Email is a method of transmitting information. It should not be considered as an area in which to store information for the long-term. Emails which are important should be saved into an appropriate storage area with other records on the same topic. This will ensure a full and complete record is kept and that emails are not ‘lost’ or hard to retrieve because they are sitting in your inbox.

Bear in mind the following key points:
- Be aware that anything you write in an email could be subject to release and compose your messages accordingly. Always consider the content and tone of your emails before you send them.
- Not all emails will be of the same importance or value to the University. Do not keep emails which have no value.
- Consider using a folder structure in your inbox to identify important emails. These can then be moved into a more appropriate storage area if required.
- If you wish to save your emails so that you can open them again as Outlook messages save them to a network drive as ‘Outlook message format’ files (.msg).
- Delete any emails which you do not need to retain. These will include emails sent for information only e.g. most CC emails (since you are not the main recipient), outdated information or personal emails.
- Manage your ‘Sent’ and ‘Deleted’ items too. The contents of these all add to the size of your mailbox.
• Clear out your ‘Deleted Items’. Anything in this box will remain there until you delete it again.
• Do not keep every email in a conversation thread unless required. If you can, simply keep the last email in the thread and delete the others.
• If you auto-archive your emails to create PST files then be aware of what you are archiving. You should weed your emails first to ensure that you are only retaining the information you require. Take into account any data protection considerations and issues around confidentiality.

RM Guidance Note: 5 Email Management

Information Security & Confidentiality
All University information should be handled according to its content and level of sensitivity/confidentiality.

It is not only good practice to apply security to safeguard the University’s sensitive/confidential information it can also be a legal requirement. One of the principles of the Data Protection Act is that appropriate security be applied when processing personal data.

To determine if information constitutes ‘personal data’ or is sensitive/confidential in a general sense you should refer to the ‘Determining if information is confidential’ document.

Key points to consider:
• Is access to the data restricted to only those staff who require it?
• Is the data secure i.e. in a locked cabinet/backed-up to a University server?
• Email should not be considered a secure mechanism for sending information. Once an email leaves the University’s system there is no control over the systems and networks it may pass through and no guarantee what might happen to it.
• Never dispose of confidential information in public places.
• Be aware of the inherent dangers in using portable media such as laptops/USB drives/CDs. These are easily lost and/or stolen.
• NEVER remove personal data from the University on any unencrypted device. If you require access to this data you should consider remotely accessing the University’s network drives. Alternatively speak to the IT Helpdesk to discuss encryption.
• Never share passwords for your personal University IT accounts with others. If you need to share information consider the other options available to you e.g. shared drive/Sharepoint/delegated access to email.
• “Lock before you walk” - always lock your workstation when you are away from your desk.
• All confidential information and/or personal data should be disposed of appropriately. Confidential waste on a variety of formats (including digital media) can be disposed securely by following University procedures http://www.strath.ac.uk/estates/recycling/atozofrecycling/confidentialwaste/

RM Guidance Note: 6 Information Security
RM Guidance Note: 7 Determining if Information is Confidential
Storing Paper Records
If you require hard copy records to be retained for the medium to long-term then you may consider depositing them in the University Records Centre. The Records Centre will accept deposits of records which require to be retained for over 12 months and are now semi-current i.e. they are not referred to on a regular basis. See [http://www.strath.ac.uk/foi/recordsmanagement/](http://www.strath.ac.uk/foi/recordsmanagement/) for further information.

The University Records Centre is only for medium-term storage and cannot accept items which need to be retained permanently. If you believe your records have to be retained permanently then you should discuss this with the University Archives. The Archives collect and preserve the institutional records and other documents which reflect the history and achievements of the University of Strathclyde and its antecedent institutions. Contact archives@strath.ac.uk for further information.

Storing Electronic Records
Electronic records, just like paper records, can be at risk of loss/damage is they are not managed appropriately. You should be aware that portable storage devices like CD-ROMS, DVDs and USB drives are not intended for long-term storage or perseveration of digital records. They are short-term storage solutions and should be used with caution.

When storing electronic records you should consider the following:

- Are you able to store records on a drive/system that is on the University’s network? Information stored on the University network is backed-up and in most cases is retrievable if accidentally deleted or there is a system failure.
- If you are undertaking a research project then check if there is a particular digital repository you must use/is recommended by the relevant funding council/research body etc. If so this is likely to have appropriate security and back-up facilities.
- The University may also require you to store research records in particular systems. Check the RKES site for more information [http://www.strath.ac.uk/rkes/](http://www.strath.ac.uk/rkes/)
- If you are using new technologies such as ‘cloud computing’ have you fully investigated the company and any associated risks with using such storage. Consider issues such as: where your data is stored, what will happen to it if the company goes bust etc. You should be aware of and consider any risks before using any such external storage facilities.
- Are you implementing a new electronic system to hold particular records? If so, have you considered what will happen to any legacy data/systems. Information that is not migrated from one system to another is at risk of obsolescene as equipment and/or software is quickly outdated and in comparatively short time electronic records may be inaccessible.
- Do you have to retain records for a significant period of time for legal/statutory requirements? If so consider how the electronic records will be managed over time. Appropriate measures will have to be taken at an early stage to ensure these records are not lost.

The issues of storing digital records and ‘digital preservation’ are complex. Given the pace with which technologies are changing the University is not able to issue technology-specific guidance as this would be quickly outdated. If you have queries about the technology you wish to use/are using then you should contact Information...
RM Guidance Note: 8 Storing Records

Retention of Information and Records
Not all records will need to be kept for the same period of time. The period for which records need to be retained will depend on legislative, statutory or operational requirements. Information should not be kept after it is no longer required.

Retaining information in any form, paper or electronic, for an extended period of time has cost implications for the University. Therefore, it is not only good practice, but it is also important for the University that records are only kept for as long as they are required. It is a legal requirement, under the Data Protection Act 1998, that personal data only be kept for as long as is required for the purpose for which it was collected. Therefore retaining personal data indefinitely ‘just in case’ could mean the University is in breach of the Act.

The University is working on producing bespoke records retention schedules to set out how long we retain different types of records for. However, in the meantime if you require guidance on how long to retain records you can refer to the JISC Infonet retention schedule for Higher Education Institutions http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-rrs-pla or contact records-management@strath.ac.uk

Some funding councils will have specific requirements relating to how long research records are retained for. You should check with your funding council for guidance. You can also read the JISC guidance on managing research records http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/managing-research-records

RM Guidance Note: 9 Records Retention and Disposal

Legislative Requirements
The University is subject to a number of ‘access to information’ regimes. These include the Data Protection Act 1998, Freedom of Information (Scotland) Act 2002 and Environmental Information (Scotland) Regulations 2004. There is a Code of Practice on Records Management under S61 of the Freedom of Information (Scotland) Act which provides a best practice framework which organisations are expected to take into consideration. The University should strive to meet this best practice.

Under the legislation mentioned above the University may be required to produce records within a statutory timeframe. To do this the University must manage its records so that the relevant records can be identified, located and retrieved when required.

The University is also subject to various other pieces of legislation that may affect its information and records management practices. You should ensure that you are aware of any relevant legislation which may affect how you manage records/what records you are able to keep/how long you are able to keep records for. Please see the ICT Legal Framework for more information.
Contacts
For more information on any of the areas listed above please contact the relevant area as listed below.

Guidance on Records and Information Management best practice (including records retention periods) contact the Records Management section (part of Information Governance and Compliance, ISD) records-management@strath.ac.uk

Technical IT issues contact the IT Helpdesk helpdesk@strath.ac.uk

Freedom of Information: foi@strath.ac.uk

Data Protection: dataprotection@strath.ac.uk

University Archives: archives@strath.ac.uk

Guidance for researchers: rkes@strath.ac.uk

Useful external resources:

JISCInfonet
Records retention - http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-rrs-pla

Guidance on Managing Research Records http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/managing-research-records

National Archives