"Records Management Good Practice Series"

Take 12 Simple Steps towards Effective Records Management

1.	When creating records, including e-mails, remember that they may be subject to Freedom of Information and / or Data Protection legislation and therefore to public disclosure.
2.	Ensure that you are creating accurate, consistent and reliable records of your business activities and decisions – think about recording basic information such as title, author, date, department or unit.
3.	Develop office filing procedures and guidelines– be consistent in approach.
4.	Paper based records, should be in a shared filing cabinet or designated area for your team. This would reduce duplication and mean all papers are easily locatable if someone is away, or if you need information on a subject that someone else is working on. Keep controls on permitted access and lock cabinets, or areas, to prevent unauthorised access or use of records.
5.	Ensure e-mails are captured and filed with the records to which they relate. Significant emails should be saved to a shared drive, University SharePoint site or Outlook folder or, if needs be, print them out and add them to an existing paper file.
6.	Name files and folders consistently and explicitly so other people can find information even if they are new or unfamiliar with the system.
7.	Maintain a list of your files and folders – keep it updated as new ones are added.
8.	Ensure facilities and equipment are suitable for the storage of records: equipment and environmental conditions should prevent damage and unauthorised access to records, while off-site storage should be similarly monitored.
9.	Electronic records should be stored on shared drives as these are backed-up on a daily basis. This will not only make it easier for colleagues who may need to access information in your absence. Do not store information on your C: drive (hard drive). IT Services are unable to backup this data and if it becomes lost or corrupted, it cannot be restored.
10.	Removable storage devices should not be used for long term storage of electronic records as they are subject to rapid technological change and obsolescence. Encrypt your data.
11.	Certain types of records, such as those containing personal data, must have specific security requirements which must be addressed by restrictions on access and use.
12.	Records should be reviewed at least once or twice a year using the institutional Records Retention Schedules, available here, as a guide as to how long to keep information. Ensure there is an audit trail of retention and disposal actions and decisions.

LM July 2017