UNIVERSITY OF
LINCOLN

University of Lincoln

Record Retention and Disposal Policy

Version 1, November 2011

Document Summary	
Author, Title and Department	**Approving Body**
Ann-Marie Noble, Information Compliance Manager, Registrar's Office	Senior Management Team
Date of Approval	**Date for Review**
28 November 2011	November 2012

Revision History			
Version	**Date**	**Author(s)**	**Note**
1	29.11.11	Ann-Marie Noble	Approved

Contents

1 Introduction

1.1 Purpose of the Policy

The University of Lincoln's Record Retention and Disposal Policy has been produced to improve the management of information and support compliance with the Data Protection Act 1998 (DPA), Freedom of Information Act 2000 (FOIA) and associated legislation. The Policy incorporates guidance from the Information Commissioner's Office (ICO), the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000, the National Archives and JISC infoNet, and has been developed with reference to the ISO 15489, International Standard on Records Management.

1.2 Policy Objectives

The objectives of the policy are:

- To improve the control of valuable information assets;
- To ensure staff manage information in compliance with relevant legislation;
- To ensure information is appropriately protected and kept secure;
- To ensure staff use information effectively and efficiently;
- To ensure the cost-effective use of physical and server space and off-site archiving;
- To ensure staff are aware of their responsibility to ensure good records management and understand that any member of staff who fails to do so may be subject to disciplinary action.

1.3 Help with this Policy

Guidance and clarification about the interpretation or any other aspect of this policy is available from the Information Compliance Manager.

2 Scope

2.1 Who is Covered by this Policy?

This policy applies to all staff at the University who create, receive and use records.

2.2 What Records Are Covered by the Policy?

This policy covers all University records, regardless of format or media.

3 The Lifecycle of Information

The University's records are important corporate assets that demonstrate its accountability, transparency and legal compliance by providing evidence of its actions and decision-making. Records must be able to be accessed when required, kept securely and disposed of appropriately when they are no longer needed.

It is important that a holistic approach is taken to managing the information contained in the University's records. This means considering the lifecycle of information and managing it accordingly during each of the following phases:

- Creation
- Active use
- Semi-Active use
- Final Outcome

3.1 Creation

When records are created they should be fit for purpose, capture relevant and reliable information and be held in an appropriate format. If the record includes personal data, staff must also ensure they are acting in compliance with the Data Protection Act and the University's Data Protection Policy.

Before new records are created consideration should be given to who will create them, where they will be held and who will have access to them. The purpose for which the record is being created should also be clear.

Records should be filed so that they can easily be located and accessed by any authorised staff. Records that are only accessible by a single member of staff, for example on their personal/'H' drive, can limit the usefulness of that information and make it difficult to respond to access requests made under the DPA and FOIA. This is particularly important for emails as normally an email inbox is only accessible by an individual user. Further information about managing emails is provided in section 5 and Appendix 1 below.

Electronic records can be held in a number of ways including on central systems such as QLS and Agresso, document management systems, PC personal and shared drives (records should not be held on PC hard drives), portable devices and increasingly on externally hosted software and web-based solutions. If personal data is being held externally it is important that this is communicated to data subjects within the relevant privacy notice when their information is collected. Further information about this can be found in the University's Data Protection Policy.

Retention periods for new records should be decided when they are created and the local record retention and disposal schedule updated accordingly. The retention period should be determined by considering the purpose for which the information is held and any legal or statutory requirements. To assist with timely disposal, for paper records, destruction dates can be stated on folders, ring binders, lever arch files or file boxes at the point the file is created. Further information about retention periods and retention and disposal schedules is provided in sections 7 and 8 below.

3.2 Active use

Once a record is created, there is normally a period when information is in constant or regular use for the purpose for which it exists. It is particularly important during this phase that information can be located quickly and easily and, for this reason, all relevant staff should be made aware of the existence of the record and how to access it.

During the active use phase there may be potential to reuse information for purposes that are beneficial for the University. However it is important to consider whether there are any barriers to re-use, for example if the information contains personal data it should not be used for a purpose that is not compatible with the reason for which it was originally collected without first notifying or seeking consent from the data subjects. Further information about sharing data between departments is available in the University's Data Protection Policy.

3.3 Semi-Active use

Records are often only in regular active use for a relatively short period of time and are then used less often. However, records tend to remain useful and may still need to be referred to in the medium term. This can be a difficult phase to manage in a structured way and there is a risk that these records will become a liability if they are not dealt with appropriately.

The point at which records move from active use to semi-active use is usually triggered by an event or milestone after which the original purpose for the record ends. At this point records should be reviewed to ensure that only information required for a defined reason is kept. For example, if records containing personal information are only required for statistical purposes, some of the personal data may no longer need to be held or it may be possible to completely anonymise the information.

This review point should also be used to consider whether other record management controls currently in place are still appropriate. For example, should access to the information be changed? does the format that the information is held in need to be altered to ensure it is preserved for the future? could the information be archived elsewhere? If the decision is taken to archive records off-site it is important that appropriate management controls are maintained as the University will still be responsible and potentially liable for the information.

Finally, if the semi active records relate to current or future records, links will need to be established so that this relationship is maintained and information is not forgotten about and can be referred to when relevant.

3.4 Final Outcome

Earlier in the life-cycle a decision should have been taken about whether the information will be preserved by the University in the long-term or disposed of at a specific point in time. If records are to be retained permanently, continued access to them must be ensured. If records are to be disposed of, this must be done so in a secure manner if they contain personal, commercially sensitive or other confidential data.

Appropriate protection methods must be used for records that are needed for future use. Where records are required in the medium and long term and are held electronically they must be protected from hardware obsolescence, software updates and storage media failure. Portable devices are at particular risk of becoming obsolete and for this reason it is not advisable to use them for the long-term storage of information. The preservation of information required in the long-term should be considered approximately every five years to ensure that appropriate actions are taken to retain access and the protection of information assets should be considered as part of risk and business continuity planning.

4 File Names and Version Control

A good file name allows not just the member of staff who created it, but any member of staff to identify its content and context without having to open it. File names should therefore be objective, meaningful, concise and standardised. The use of established naming conventions also helps identify documents for disposal and reduces the risk of accidently destroying information.

It is important that it is always clear which is the most recent version of a document and whether a document is draft or final. This can easily be done by using version coding in file names and text watermarks. Although there are many different version coding conventions, a particularly simple one is to number a first draft ‘v0.1’ with changes to it numbered ‘v0.2’ and so on until a final version is agreed and numbered ‘v1’. If changes are made to the final version over time the number changes to ‘v1.1, v1.2’ etc. If the document is substantially changed it may be appropriate to show this by numbering it ‘v2’.

When there are multiple versions of a document a decision to either destroy or keep previous versions needs to be made. Retaining previous or draft versions can sometimes be useful or even necessary. However, where this is done their draft or superseded status must be clear and it should be noted that the FOIA covers all information held.

Document control sheets are useful for recording the review and release of formal University documents like policies. A control sheet contains details of the revision process including who made the revisions and why. An example can be found on page 2 of this policy.

It is also preferable to control the number of copies of a document in circulation. It is a good idea to refer people to a single version, for example posted on the Portal, to ensure the most up to date version is being used. Where a number of staff members on a shared network area are working on a document, using the ‘Insert Hyperlink’ function within Microsoft Outlook provides a live link to a particular copy of the document for editing.

5 Email Management

Emails form part of the University’s records and it is important that they are managed effectively as they could be requested under the DPA or the FOIA. Appendix 1 of this policy provides some good practice advice about managing email. It is recommended that staff do not use personal email accounts for conducting University business and staff should be aware that if they do, information contained in relevant emails may still be subject to disclosure.

The University has an Email Archiving System which automatically archives all emails after a certain period of time. The purpose of the system is to improve the administration of the email service by storing archived emails in a different way. However, the system is not intended to be a records

management tool and staff remain responsible for actively managing any emails that are held in the archive.

Staff are expected to ensure that email is used in a secure way when necessary. Email security is covered in the University's Information Systems Acceptable Use Policy and Data Protection Policy.

6 Information Access and Security

It is often necessary to control access to information, for example to protect the commercial and intellectual assets of the University, the personal data of individuals and the interests of third parties. Therefore, personal, commercially sensitive or otherwise confidential information must be held securely. Information security is covered further in the University's Information Systems Acceptable Use Policy and Data Protection Policy.

A clear understanding of the business processes for which the information is to be used will be instrumental in ensuring an appropriate level of access is maintained. Careful consideration is required to ensure that the right balance is struck between open access and security to ensure that only the right people have access to the right information.

7 Record Retention Periods

Establishing retention periods should ensure that records are not mistakenly deleted too soon or kept for too long. When determining retention periods, both internal and external factors may need to be taken into account. Internally, the length of time information is required for operational needs will be determined by the purpose for which the information is held and any secondary purposes. External factors will mainly be related to legal and regulatory requirements but in some cases may also be determined by audit requirements or contractual obligations with external organisations. Where information is shared between University departments, retention periods should be agreed between parties to ensure consistency.

8 Record Retention and Disposal Schedules

All departments are required to keep and maintain a local record retention and disposal schedule. A template and further guidance is provided by the Information Compliance Manager.

A local record retention and disposal schedule should list the electronic and paper records held by the department and specify their retention periods. Departments should review their local schedule regularly and ensure that records are disposed of appropriately and in accordance with the specified retention timescales.

Record retention and disposal schedules help departments to confidently dispose of records when they are no longer required and ensure that records are disposed of consistently no matter where they are held. The value of the information to the University should justify the cost of the continued retention as storing records unnecessarily can be expensive in terms of staff time, space and equipment. It can also create liabilities due to the need to respond to information requests made under the DPA and FOIA and there is a risk of non-compliance with the DPA if personal data is kept for longer than is necessary. Furthermore, the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000, forms a requirement to establish records management systems and procedures. While the provisions of the Code aren't mandatory, failure to comply may be seen as indicative of failure to comply with the rest of the FOIA.

Email Management: Good Practice Guidance

General

Although email is invaluable for work, the large volume of emails received can make it difficult for staff to deal appropriately with messages as and when they arrive. Therefore, instead of either acting on the email and deleting it or filing it appropriately, messages tend to accumulate unmanaged within users' inboxes. It is however the responsibility of all staff to manage their mailboxes appropriately and time should be allocated for this purpose. Staff may find the following approaches helpful:

- Give emails meaningful titles to help file and locate them more easily.
- Restrict emails to one subject. This will make them easier to file and dispose of and will reduce the risk of confidential or sensitive information being inadvertently disclosed.
- If the subject of a string of emails significantly changes, start a new email message, copying relevant sections from the previous string.
- If emails are required for future use or reference, save them in the relevant manual or electronic file and delete the message in the mailbox. This will also help ensure that emails are kept in line with any retention periods stated in the local retention and disposal schedule.
- Be clear about whether an email requires action or is only for information.
- Only distribute email messages to the people who need to know the information. For instance, only use the reply all facility if everyone needs to know your reply.

In addition to the above, Microsoft Outlook provides email management tools which staff may find useful. The University provides on-line IT training on as part of it staff development and training programme if staff wish to learn more.

Confidential Subjects and Email Security

When dealing with confidential or sensitive issues, sometimes it can be more appropriate to speak to someone in person or by telephone (if necessary you can place a factual note regarding the conversation on file). This reduces the risk of the information being accidently disclosed if emails are forwarded or viewed by anyone other than the intended recipient. In addition, copies of emails can be required under the DPA or FOIA. In general, avoid putting anything in an email that you wouldn't put in a letter.

Care should also be taken when using the reply all or forwarding functions or copying others in to emails. Consideration of who needs to know what will not only help to reduce the volume of email traffic but will help ensure that personal data or other confidential information isn't inadvertently disclosed. Use of the blind copy facility should be considered when sending an email to multiple people to avoid disclosing personal information to other recipients, for example personal email addresses or other information that could be deduced simply by their inclusion in the email distribution.

It is important to ensure that emails are correctly addressed, particularly when sending personal data or other confidential information. Any disclosure of personal information to unintended recipients may constitute a breach of the DPA and should be immediately reported to the Information Compliance Manager. To help reduce the risks associated with inappropriate disclosure, only send the minimum amount of information required, make it clear when sending confidential messages that the content is sensitive and consider appropriate security methods. Remember when sending messages to external email addresses that email is not a secure method of communication. This means that sending personal data via external email should be avoided unless it is encrypted.

Sources of Further Advice and Guidance

University Staff

Records Management, Data Protection and Freedom of Information
Information Compliance Manager, email: compliance@lincoln.ac.uk

Information Security
Information Security Manager, email: infosec@lincoln.ac.uk

Related University Documents

Local Record Retention and Disposal Schedules – Guidance and Template
Available via the Portal at https://portal.lincoln.ac.uk/C18/FreedomOfInformation/default.aspx

Data Protection Policy
Available via the Portal at https://portal.lincoln.ac.uk/C10/C10/DP/default.aspx

Information Systems Acceptable Use Policy
Available via the ICT's Portal pages at https://portal.lincoln.ac.uk/C2/C5/ICTPolicies/default.aspx

External Links

Advice from the Information Commissioner's Office on records management is available on its website at http://www.ico.gov.uk/for_organisations/freedom_of_information/records_management.aspx

The 'Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000' is available on the Ministry of Justice's website at http://www.justice.gov.uk/guidance/docs/foi-section-46-code-of-practice.pdf

The National Archives provides guidance on records management guidance and on the Lord Chancellor's Code of Practice on its website at http://www.nationalarchives.gov.uk/information-management/

JISC infoNet provide a Records Management infokit on its website at http://www.jiscinfonet.ac.uk/infokits/records-management