Records Management Policy

Document Control	
Owner:	Natasha Lock, Information Compliance Manager
Contact:	Compliance@lincoln.ac.uk
Version number:	V2.0
Approval date:	23 September 2024
Approved by:	Senior Leadership Team
Date of next review:	September 2026

1. Purpose

1.1 The University of Lincoln's Records Management Policy's aim is to foster an enhanced information management culture focusing on the management of personal information handled by the University. Implementation of this policy will support compliance with UK legislation relating to personal data, particularly the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000 (FOIA) and associated legislation including The UK Data Protection Act 2018; the legislative environment supporting the need for this policy is described in Annex A and includes a summary of the UK GDPR Data Protection (DP) Principles.

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 FOIA ('the Section 46 CoP'), the National Archives and Jisc InfoNet. It has been developed with reference to ISO 15489, International Standard on Records Management.

1.2 Policy Objectives:

- To ensure staff manage information in compliance with relevant legislation;
- To improve the control of valuable information assets;
- To ensure information is appropriately protected and kept secure;
- To ensure staff use information effectively and efficiently;
- To ensure the cost-effective use of storage, including 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.

2. Scope

2.1 This policy applies to all staff members of the University.

2.2 The Section 46 CoP defines 'records' as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. This policy covers all University records, regardless of format or media.

3. Roles and Responsibilities

3.1 All University staff and students are required to adhere to this policy.

3.2 The Data Protection Officer is responsible for promoting and ensuring good records management practices at the University.

4. 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 a holistic approach is taken to managing the information contained in the University's records, by considering the lifecycle of information and managing it accordingly during each of the following phases:

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

4.1 **Creation**. When records are created, they should be fit for purpose, capture relevant and reliable information, and be held in an appropriate and secure format. 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. If the record includes personal data, staff must also ensure they are acting in compliance with Data Protection (DP) Legislation (including the UK GDPR DP Principles) and the University's Data Protection Policy. The purpose for which the record is being created should also be clear, and the legal basis for processing any personal data must be recorded. At this stage it is important to consider whether the purpose is compatible with the purpose for which any personal data was collected, and to issue a new privacy notice to individuals if it is not. The Information Compliance Team can advise in case of doubt.

Records should be filed so they can easily be located and accessed by any authorised staff. Records 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 DP legislation and FOIA. Therefore, all personal and institutional data must be stored in the University data environment and should not be stored on personal drives. This is particularly important for email as normally an email inbox is only accessible by an individual user. Further information about managing emails is provided in Section 6 and Annex B below.

Electronic records can be held in several ways including on central systems such as OneUni, on shared computer drives, on portable devices and increasingly on externally hosted software and web-based solutions. If personal data is being held or processed outside the University, this must be notified to data subjects within the relevant privacy notice provided when their information is collected. Further information about data sharing and privacy notices can be found in the University's Data Protection Policy or by contacting the Information Compliance Team.

Retention periods for new types of records should be decided when they are created and the Records Retention Schedule updated if necessary, including communication to the Information Compliance Team. The retention period should be determined by considering the purpose for

which the information is held and any legal or statutory requirements. Retention of records beyond the planned retention period may breach DP legislation; this means that a disposal mechanism must be arranged for each type of record within each department. 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, and some electronic storage systems have an automatic deletion capability. Further information about retention periods and retention schedules is provided in Sections 8 and 9 below.

4.2 **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 beneficial to 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 and perhaps seeking consent from the data subjects.

4.3 **Semi Active-Use.** Records are often only in regular active use for a relatively short period of time and are then used less often but may still 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 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 (for example, the end of an academic year). At this point records should be reviewed to ensure 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 and can be deleted 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 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 appropriate management controls are maintained as the University will still be responsible and potentially liable for the information; a data processing agreement will certainly be needed.

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

4.4 **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 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 appropriate actions are taken to retain access. The protection of information assets should be considered as part of risk and business continuity planning.

5. File Naming Conventions and Version Control

A good file name allows 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.

Consideration should be given to agreeing a standardised file naming convention within each work area or department. The following guidelines are recommended for use throughout the University, but it is recognized there may be other protocols in use that meet business needs in some areas.

The naming convention must be adopted when the document is first created, and the filename and path should be included in the footer of the document. Key considerations for your naming convention should be:

- File names should be short, but meaningful;
- Indicate separate words with capital letters rather than spaces, underscores, or full stops;
- If the date is included in the filename, it should be in the format YYYYMMDD or YYYYMM or YYYY-YYYY (for chronographic listing);
- Avoid using non-alphanumeric characters in file names as these may be problematic in some systems, e.g. SharePoint;
- Be wary of including acronyms in the filename as these may not be as obvious over the full lifetime of the document; this may be dealt with by use of named folders with an explanation or an index file.
- Order the elements in the filename as appropriate for retrieving them – this will vary with business area;
- Avoid using common words (e.g. draft or final) at the start of filename unless needed for retrieval;
- Numbers included should always have at least two digits, unless a year, e.g. 02
- Personal names should be in the format family name followed by initials with no commas, e.g. BloggsJO;
- For documents that relate to recurring events, ensure the date is included in the filename.

5.1 **Version numbers.** To make it clear which is the most recent version of a document and whether a document is draft or final, use 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 must be made to either destroy or keep previous versions. 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 of document control can be found on Page 1 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 or on OneDrive/Teams, 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; OneDrive or Teams can also be used in Office 365 to allow a number of people to edit documents collaboratively and maintain version control automatically.

6. Email Management

Emails form part of the University's records and it is important they are managed effectively as they could be requested under Data Protection legislation or the FOIA. Annex B of this policy provides some good practice advice about managing email. **Staff are not to use personal email accounts or personal social media accounts for conducting University business**. Staff should be aware that if they do, information contained in relevant emails or messages may still be subject to disclosure, and that any such use of these systems may not be compliant with data protection laws.

The University has an Email Archiving System which automatically archives all emails after two years 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 email is used in a secure way when necessary. Email security is covered in the University's ICT Acceptable Use Policy and Data Protection Policy.

7. 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 ICT Information Security Policy, the University 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 the right balance is struck between open access and security to ensure only the right people have access to the right information.

8. Records Retention Periods

Establishing retention periods should ensure records are not mistakenly deleted too soon or kept for too long. Personal data must not be retained for longer than needed, unless they are to be archived in the public interest, or for scientific or historical research purposes or statistical purposes.

When determining retention periods, both internal and external factors must be considered. 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, and to ensure multiple copies are not retained. Additionally, the University accepts payment by card but does not hold or retain any payment card data.

9. Records Retention Schedule (RRS)

Records retention and disposal schedules help departments to confidently dispose of records when no longer required and ensure records are disposed of consistently no matter where they are held. The value of retained information should justify the cost of continued retention as storing records unnecessarily is expensive in terms of staff time, storage space, and equipment. Retained data may need to be disclosed under subject access rights and FOIA, which may result in extra work if more data has been retained than necessary. There is also a risk of non-compliance with data protection legislation if personal data is kept for longer than necessary.

Additionally, the Lord Chancellor's Code of Practice on the Management of Records issued under Section 46 of FOIA requires the University to establish records management systems and procedures. While the provisions of the Code aren't mandatory, failure to comply may be seen as an indication of failure to comply with the rest of the FOIA.

In consultation with all departments, the University has created a Records Retention Schedule (Annex C) which states and explains the rationale behind the retention period for different types of records, and makes it clear what the disposal schedule for records should be. All departments are required to adhere to this schedule. If a variation to the Schedule is required, this should be advised to the Information Compliance Team. Where the University Records Retention Schedule does not explicitly state the retention period for a particular type of record, the Jisc model Records Retention Schedule will apply (Annex D), but it is recommended departments consider adding this type of record to the University Schedule making any adjustments necessary for local circumstances.

The Records Retention Schedule should list all types of electronic and paper records held by the department and specify their retention periods. Departments should ensure records are disposed of appropriately, securely and in accordance with the specified retention timescales.

Annex A
Legislative Obligations for Managing Records

A.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is EU (European Union) legislation that has direct effect in the UK and was enforceable from 25 May 2018. The GDPR aims to protect the personal data of EU/UK citizens and give them more control over how their data is used. It also aims to harmonise data protection laws across Europe and to ensure organisations take a more responsible approach to data privacy, especially as technological developments make it easier to process data on larger scales. Post-Brexit, the UK has enacted GDPR into UK law, ensuring it is applicable beyond the UK's membership of the EU, and has been named the 'UK GDPR'.

The GDPR imposes constraints on how personal data can be 'processed', which includes but is not limited to: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR sets out six main data protection (DP) principles for the processing of personal data stipulating that personal data should be:

(a) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency'),
(b) collected for specified, explicit and legitimate purposes ('purpose limitation'),
(c) adequate, relevant and limited to what is necessary ('data minimisation'),
(d) accurate and where necessary kept up to date ('accuracy'),
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed ('storage limitation'),
(f) and processed in a manner that ensures appropriate security of the personal data ('integrity and confidentiality').

An additional principle of accountability is central to GDPR, requiring that organisations must be able to demonstrate their compliance with the data protection principles to individuals and the regulator, the Information Commissioner's Office (ICO). The four DP principles of data minimisation, accuracy, storage limitation and integrity and confidentiality are all pertinent to records management, and good records management is essential to be able to comply with the accountability requirement.

A.2 Freedom of Information Act 2000 (FOIA)

The Freedom of Information Act 2000 (FOIA) gives members of the public the right to access information held by public authorities and places a duty on these authorities to make available the information they hold. FOIA aims to increase the openness, accountability and transparency of public authorities. In Section 46 of FOIA, there is allowance for a code of practice to be issued to give guidance on good practice in connection with "the keeping and management and destruction of their records". The Lord Chancellor's Code of Practice on the Management of Records was issued under this section of FOIA ('the Section 46 CoP').

Annex B
Email Management: Good Practice Guidance

B.1 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 in filing and locating – use the file naming convention.
- Restrict emails to one subject, reducing the risk of accidental disclosure of information to the wrong party;
- If the subject of an email string changes, start a new email message, copying relevant sections in if required;
- If the email is required for future use or reference, save them in a relevant file and delete the message in the mailbox (this helps in complying with retention schedules)
- Be clear whether an email requires action or is for information only;
- Only distribute email messages to the people who need to know the information, taking particular care with the use of 'reply all';
- Check out the email management tools in Outlook as they can help you automatically manage your email;

B.2 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 into emails. Consideration of who needs to know will not only help to reduce the volume of email traffic but will help ensure personal data or other confidential information isn't inadvertently disclosed. Mail merge or secure data transfer services should be used when sending emails to multiple people to avoid disclosing personal information to other recipients. The use of BCC is not advised due to being one of the most common personal data breach causations.

It is important to ensure emails are correctly addressed, particularly when sending personal data or other confidential information, and Digital Technologies guidance should be followed. Any disclosure of personal information to unintended recipients may constitute a breach of the DPA and should be immediately reported to the Information Compliance Team. 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. Personal Data should be sent via secure links where applicable, such as OneDrive, or password protected/encrypted. You should not send personal data via email if it is not protected.

Annex C
Records Retention Schedule

The University of Lincoln Records Retention Schedule can be accessed via this link:
UoL Record Retention Schedule

Annex D
Jisc Records Retention Schedule

The Jisc Records Retention Schedule can be accessed via this link:
records-retention-management-spreadsheet.xlsx (live.com)

Additional information about the Jisc RRS can be reached via this link:
Records retention management - Jisc

Annex E
Sources of Further Advice and Guidance

University Staff

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

Digital Security
Digital Security Manager, email: dt@lincoln.ac.uk

Related University Documents

University of Lincoln Records Retention Schedule
Available via the Portal at: UoL Record Retention Schedule

Data Protection Policy
Available via the Portal at: UoL Data Protection Policy

Digital Technologies Acceptable Use Policy
Available via the Digital Technologies Portal pages at: University Acceptable Use Policy

External Links

Advice from the Information Commissioner's Office on records management is available at: https://ico.org.uk/media/for-organisations/documents/1624142/section-46-code-of-practice-records-management-foia-and-eir.pdf

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 at: https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf

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

Jisc provides Records Management guidance on its website at:
https://www.jisc.ac.uk/guides/records-management