Records Management Policy

Document Control	
Document Type:	Policy
Department:	Legal & Governance
Relevancy:	Group-wide
Owner:	Lucynda Kelman, Assistant Data Protection Officer
Approver:	Executive Team
Published Date:	
Version:	1
Security Classification:	Internal
Last Review Date:	22/09/2021
Next Review Date:	22/09/2022

Contents

Related documents

- **Data Retention Schedule**
- Data Asset Register
- ITS049 Information Retention Policy
- Acceptable Use Policy
- Data Protection Policy
- Safeguarding Policy
- IT Usage Policy

Purpose

LTE Group recognises that efficient record management is essential to comply with legislative, regulatory, funding, and ethical obligations, to support our core function and enable the effective management and administration of our services.

Efficient records management enables the LTE Group, and its operating divisions, to meet the following objectives:

- Adhering to legal, regulatory, funding, and ethical obligations
- Adhering to disclosure requirements under the Freedom of Information Act 2000
- Maintain authentic, accurate, reliable, and good quality records
- Ensure records can be easily found, accessed, and understood by those who need them
- Efficient use of physical and server space

This policy outlines LTE Group's framework for records management, roles and responsibilities, periods for retention, and advice on destruction.

Scope

This policy applies to all active and archived records created, captured, maintained, used, or destroyed by LTE Group, and its subsidiary companies, in the course of its core activities in relation to the delivery and administration of its services.

This policy applies equally to all records that are created and held, both in electronic and paper format.

This policy is supplemented by the **Data Retention Schedule,** which is based on the JISC model retention schedules for Further & Higher Education, as well as guidance on employee records published by the Chartered Institute of Personnel and Development. If you have any questions regarding information that falls outside of the **Data Retention Schedule** or this policy, please contact the Data Protection Officer at dpo@ltegroup.co.uk

Responsibility

The Assistant Data Protection Officer has overall responsibility for this policy and its implementation.

Senior leadership and management will have overall responsibility for their department's data retention management, and it is their responsibility to ensure all staff are adequately trained and made aware of the key principles of this and related policies.

All LTE Group colleagues are responsible for ensuring that data and information is recorded, handled, and destroyed in line with this policy. Colleagues can assist with the implementation of effective records management by:

- Creating and maintaining a full and accurate record of your activities;
- Following the team's agreed filing procedures;
- Listing files as they are created and keeping the list up to date;
- Regularly reviewing and disposing of files according to the **Data Retention Schedule**;
- Keeping files neat and tidy and not letting filing backlogs build up;
- Being aware and mindful that the public may request to see LTE Group's records under the Freedom of Information Act 2000 and the Environmental Information Regulations. Records might also be subject to disclosure as a result of data subjects' rights under the General Data Protection Regulation (GDPR) (Subject Access Request).

Compliance with this policy is mandatory and relates to all departments in LTE Group and any subsidiary companies.

Records management

Filing and storage

All records should be kept in appropriate and secure storage during their active lifecycle.

Ideally email should not be used for storing important records. Emails that constitute a record which needs to be retained, including those containing personal data, should be

stored in an appropriate filing system relevant to their confidentiality or criticality. In any case, any data held within email systems must be managed in accordance with the **Data Retention Schedule**.

Shared drives or other unstructured information storage solutions (including SharePoint and cloud-based storage) used to store any record should be managed in accordance with the **Data Retention Schedule**, and records should be filed under an appropriate folder structure within those systems.

Filing systems should be structured so that they facilitate the application of the **Data Retention Schedule**. An example of this would be the filing of record types by year to facilitate annual destruction cycles.

Master Records	Master records are definitive copies of documents (or spreadsheets, databases, presentations, images, sound recordings, etc.) held by the 'Records Owner'. The Records Owner is either the originator of the master record or the current member of staff who is formally responsible for the master record as part of their duties.
Duplicate records	During the retention period, only one copy of each record (the master record) needs to be kept for the full length of this period. Duplicate and secondary copies should be destroyed as soon as they are no longer of immediate operational use. Duplicate records should not be kept for longer than the appropriate retention period.
Transitory Records	Transitory records are records which have no significant ongoing value after they have served their primary purpose. Some examples of Transitory Records are: • Draft documents and working materials which do not demonstrate significant steps in the development of a final version; • Documents containing requests for information which have no further value after the information is provided or received; • Items received only for information from elsewhere in LTE Group, often as part of a distribution list; and • Items received only for information from external organisations. It is recommended that, when no longer required, Transitory Records should be destroyed in the normal course of business.

Yearly cycles

There can be some confusion as to whether 'year' relates to the UK fiscal year, the College financial year, the 'academic' year or the calendar year.. For all business areas, LTE Group recommends that the yearly destruction cycle be completed in line with the calendar year, so over the months of December and January. This allows any data destruction activity to take

place once per year, meaning that there is no expectation for departments to continually monitor retention/destruction practices in-year.

Retention

The Data Protection Act (2018) and GDPR sets out seven key Principles that LTE Group, as a data controller, must follow. One of these Principles relates to storage limitation. This means that we should not hold personal data for longer than we need it.

LTE Group retention periods are set out in the **Data Retention Schedule,** which specifies obligations to destroy information after the retention period has ended.

The majority of records will eventually be destroyed, however, there are a small number of records and artefacts that are deemed to be of permanent legal or historical significance that will be preserved in LTE Group's electronic or manual archive facilities.

Retention periods will consider the following:

- Any legal or contractual requirements;
- An assessment of the value of the information, taking into account the need for evidence processes, the probability of future uses and the consequences of not having the information available;
- A consultation with the owner and users of the records, where appropriate;

Retention periods should remain the same for the same type of recorded information, regardless of what media they are stored in, i.e. information should be kept for the same period of time whether they are in digital or paper format. It is not necessary to retain duplicate copies – either digital or paper will suffice, not both.

The principle underpinning these requirements is the recognition that holding recorded information is an active, not a passive process. It involves the exercise of responsibility in the same way as destroying it, acquiring it, or creating it.

Destruction

Destruction obligations apply equally to paper and electronic records. The **Data Retention Schedule** is structured so that destructions become due at the end of an academic year, this allows one destruction exercise to be conducted once per year.

Paper records should be placed in confidential waste bins for secure destruction. This facility is provided by an external confidential waste facilitator, Shred-It, and multiple confidential waste bins are located across all LTE Group sites.

Any issues concerning the destruction of paper records should be directed to dpo@ltegroup.co.uk

External records should be securely deleted. Backups of IT systems containing electronic records for disaster recovery purposes are not deemed to be active records. Therefore, electronic records are considered to be 'destroyed' when the Records Owner performs the deletion.

If, at the end of the retention period, it is technically or administratively impossible to delete or destroy a local record, then the Data Protection Officer should be informed. The Assistant

Data Protection Officer will then perform an exception process and risk assessment and advise accordingly.

Any issues concerning the destruction of electronic records should be directed to the Information Services (IT) help desk, via the LTE Group Self-Service Portal.

External storage (and destruction of records)

- Our external archive for paper records is currently an external agency, DeepStore
- Related records are archived in boxes which are internally referenced by LTE Group (or any subsidiary companies) and given a bar code identifier by DeepStore
- The Senior Administrator within Planning & Performance (TMC) holds a central register of the documents that have been transferred to DeepStore
- Documents can usually be retrieved within 3 working days (or up to 5 working days for more than 50 boxes)
- When the destroy date is reached, DeepStore will supply a Destruction List to LTE Group (and subsidiary companies) which must be approved and returned by LTE Group (or subsidiary companies) before any of the archived records are destroyed. Records are not routinely destroyed upon reaching the initial destroy date
- Electronic records will be destroyed/deleted when the destroy date is reached

Total People

Total People external records storage facility are provided by Deadfiles Facilities Ltd (L&R Storage). Deadfiles will provide archiving boxes to Total People, for external archiving of records. Deadfiles will collect the records from Total People premises on request from a department.Upon receipt of the records into Deadfiles facility, Deadfiles will provide Total People with a Client File Record in respect thereof.

Access to the records at Deadfiles facility is limited to named colleagues within Total People. Records may be retrieved from storage individually, or in complete boxes. Records will usually take up to one working day to be retrieved and provided to Total People.

Where records entering the Deadfiles facility have a review or destruction date indicated on the cover sheet, this will be noted by Deadfiles and Total People will be notified in advance of any upcoming review or destruction dates. Deadfiles can arrange for destruction, on behalf of Total People and only on the instruction of an authorised, appropriate signatory.

Back-up

LTE Group regularly backs up critical data, to allow it to be accessible and restorable in the event of an incident occurring. Therefore, for each critical LTE Group system or application, the system owner should define (to Information Services) what information is to be backed up and the expected / required maximum retention for any information being backed up. The maximum retention for electronic back up (via tape, non-editable media) is usually 10 years. The system owner should notify Information Services on items requiring shorter retention

periods than this to allow us to demonstrate compliance against retention, however it is noted that once information reaches this stage (back up via tape) LTE Group considers this information as 'beyond use' as it is no longer accessible to system owners or colleagues and is defined as non-editable media.

Departmental Procedures

Some business units and departments have their own procedures and should be referred to where appropriate. These are outlined below.

Department	Procedures
Finance	Records are retained on site until the annual audit is completed and then sent to the external archive for storage.
Information Services	LTE Group Information Services undertake records management under their own policy, in line with their ISO27001 accreditation. ➢ ITS049 Information Retention Policy
Novus	Novus undertake records management under their own scheme and policies: ➢ NOV016 Novus Data Retention, Archiving & Disposal Policy ➢ NOV045 Novus Retention & Archiving Guidance