



UNIVERSITY OF LINCOLN

ICT Services Data Retention Policy

Author	Martin Coulson, Information Security Manager
Approved	D Cook
Current Version	1.2
Issue Date	02/8/2019
Review Date	1/7/2020

Revision History

Version	Date	Author(s)	Notes on Revisions
0.1	16/10/15	Mark N R Smith	Initial draft
0.2	11/12/15	Mark N R Smith	Amendments from DC
0.3	16/12/15	Mark N R Smith	Further amendments from DC
0.4	25/1/15	Mark N R Smith	Comments from Security Group
0.5	27/04/16	Drew Cook	Changes to section 5 with regard to retention of personal data, operations management information and asset information.
1.0	6/07/16	Mark N R Smith	Issued as version 1.
1.1	02/08/18	Martin Coulson	Inclusion of GDPR reference
1.2	02/08/19	Martin Coulson	Updated the JISC link in Section 2, regarding Records Retention Management.

Approval

This document has been approved by:

D Cook – Director of ICT

Signed:	Date:
----------------	--------------

Contents

1	Introduction	4
2	Background	4
3	Scope	4
4	Objectives	4
5	Categories of ICT Services Data	5
5.1	ICT Services Data with Statutory Retention Periods	5
5.2	ICT Services and Personal Data	5
5.3	ICT Services and Freedom of Information Data	6
5.4	ICT Services Commercial and Contractual Data.....	6
5.5	ICT Services Student Relationship Management Data	6
5.6	ICT Services Backup Data	7
5.7	ICT Services Legacy Computer Equipment	7
5.8	Miscellaneous ICT Services Data	7

1 Introduction

This document sets out the policy for how long ICT Services must retain data and when data should be disposed of.

This policy is intended to implement the statutory legal and regulatory requirements to both keep and dispose of data appropriately taking into account of the business needs of ICT Services providing services to the wider University.

This policy categorises types of ICT data according to its respective retention and disposal requirements and describes these requirement for each.

2 Background

The retention periods here are based on the JISC Record Retention Schedule found at: <https://www.jisc.ac.uk/guides/records-retention-management>. These take account of the legal requirements and best and common practice for universities and organisations in general.

Many UK Universities have produced an overall Record Retention Policy which includes the specific ICT Services data elements mentioned below. This policy highlights the items that apply to ICT Services showing their required retention period.

3 Scope

This policy applies to data that ICT Services owns as opposed to data for which ICT Services is the custodian of on behalf of other areas of the University. Provisions in this policy will also apply to other areas of the University and it is expected that the University areas outside ICT Services in conjunction with ICT Services will implement similar policies to this for data in the custody of ICT Services.

This policy applies to all information held by ICT including traditional data held electronically as well as information held on paper and any other media. This includes all files, emails, images, audio, video and backup data that may be held by ICT Services.

This policy applies to all ICT Services staff at the University of Lincoln.

4 Objectives

The aims of this policy are to:

- Prevent the premature destruction of data that needs to be retained for a specified period to satisfy legal, financial and other requirements of ICT Services and the wider University

- Provide guidance to ICT Services staff implementing processes and procedures to manage the lifecycle of data used to provide ICT services
- Provide consistency for the destruction of data no longer required after specified periods
- Promote improved data management practices within ICT Services

5 Categories of ICT Services Data

The following categories of data held by ICT Services are set out below. Firstly, some data has statutory retention periods.

5.1 ICT Services Data with Statutory Retention Periods

The majority of types of University data that has statutory retention periods is not held on behalf of ICT Services. These relate to health and safety, accidents, sickness, financial, tax and payroll records.

The main area that concerns ICT services is the obligations under the EU Hazardous Substances in Electrical and Electronic Equipment Regulations (RoHS Regulations 2008). ICT disposes of unwanted electrical and electronic equipment through a third-party contractor. The RoHS regulations require that organisations keep a record of disposal of electrical and electronic equipment – **retain 4 years**.

5.2 ICT Services and Personal Data

The General Data Protection Regulation (GDPR) [article 5, clause 1(e)] states that personal data should not be kept for any longer than necessary and should be removed when it is no longer needed.

According to the regulator the ICO this means that ICT Services must:

- Review the length of time ICT Services keeps personal data;
- Consider the purpose or purposes ICT Services holds the information for in deciding whether (and for how long) to retain it;
- Securely delete information that is no longer needed for this purpose or these purposes; and
- Update, archive or securely delete information if it goes out of date.

ICT Services uses Personal Data for its own purposes in the following areas:

- ICT Service Desk – The personal data of staff is retained by the University whilst they are employed at the University and for a period of 1 year after leaving the University
- ICT Service Desk – The personal data of students is retained by the University whilst they are enrolled at the University and for a period of 1 year after leaving the University

- ICT Information Services – small samples of Personal Data used for system development, fault diagnosis and testing – **retain only while being used and destroy immediately after**
- ICT Services – data recorded, notes etc. about health matters as part of pastoral care, return to work interviews etc. by line managers and team leaders – **retain whilst the member of staff is employed by the University. Once the member of staff ceases being employed by the University retain for a further year, if there are any ongoing discussions or procedures in progress at the time employment ceases retain until completion of the procedures/discussions plus 1 year.**
- ICT Technical Services – Video clips recorded by the Data Centres to monitor the critical infrastructure – **retain 6 months from date of recording**. Clips used for an investigation should be **retained for six years after the investigation is concluded.**

5.3 ICT Services and Freedom of Information Data

It is an offence under the Freedom of Information Act 2000 to destroy records in response to a FOI request. This policy avoids any misunderstandings that may arise from the arbitrary destruction of data.

5.4 ICT Services Commercial and Contractual Data

ICT Services uses third-party suppliers to deliver services that are governed by contracts. The specification and development contracts and the evaluation of suppliers may be challenged at a later date so this data must be retained.

These are:

- Pre-contract advice – **2 years**
- Specification and contract development – **6 years after contract expires**
- Evaluation of tenders – **6 years after contract expires**
- Unsuccessful tender documents – **1 year after contract starts**
- Post tender negotiation – **1 year after contract starts**
- Contract Management – **2 years after contract expires**
- Contract amendments – **6 years after contract expires**

5.5 ICT Services Student Relationship Management Data

ICT Services engages with students to seek direction and feedback about current, developing and potential services. This may occur on a regular basis or as part of specific service related initiatives.

Any Personal Data in the context of student relationship management is covered by section 5.2 above. It is recommended that relationship management data be anonymised within 3 years after it is collected but the anonymised information may be retained as long as required for longitudinal analysis.

5.6 ICT Services Backup Data

ICT Services backs up data on behalf of schools and departments across the University. The retention periods for this data are expected to be covered by Data Retention Policies for these departments. However ICT Services also backs up data in relation to its own work as building, changing and testing services and databases – this is considered ICT test data.

If test data is copied from live systems or otherwise includes live data the preference is to anonymise, redact or replace any personal data. If this is not possible then personal data in test systems should be treated as described in section 5.2.

It is expected that this data is deleted and destroyed immediately it is no longer required or in any event – **within one year**.

5.7 ICT Services Legacy Computer Equipment

ICT Services obtains computer equipment that has reached the end of its service life and has been replaced. These computers often contain storage devices or disks which may contain data from the school or department that used them.

ICT Services securely stores this equipment until it is recycled by a third-party recycling organisation. From the date the recycling company receives the equipment the data on these computers will be destroyed – **within 28 days**.

5.8 Miscellaneous ICT Services Data

Other ICT Services data not covered by the categories above are listed below:

- ICT service and systems development – **retain 5 years after last development action**
- ICT Operations management **retain for the period of the current strategic plan plus 2 years**
- ICT Incidents & Service Requests – **retain for the life of the relevant asset plus 1 year or 5 years whichever is the longest**
- Software licenses – **retain until new license issued or until license expires and software ceases to be used and is removed from all systems**
- User account changes – **retain until closure of account plus one year**
- Security incidents and action taken – **retain for the life of the relevant assets plus 1 year or 5 years whichever is the longest**
- Third-party network connections – **retain one year after connection terminated**

- Specification and selection of major assets – **retain life of asset plus 6 years**
- Specification and selection of other assets – **retain life of asset**
- Maintenance information of major assets – **retain 6 years after decommissioning**
- Asset configuration management information- retain for life of asset plus 1 year