

# Records Retention and Disposal Policy

---

## 1. Introduction

This policy sets out the University of Nottingham's definition of, commitment to and requirements for the retention and disposal of records. It sets out the need to understand the nature of the records created and held by the organisation and the requirements for the retention and disposal of each.

This Records Retention and Disposal Policy provides management direction and support for the retention and disposal of records across the University. It is applicable to, and should be communicated to, staff, students and other relevant parties.

## 2. Purpose

The aim of this policy is to ensure that records are managed consistently across faculties and departments, that they are retained for sufficiently long to meet operational and business needs, and demonstrate compliance with legal, regulatory and audit requirements, and thereafter disposed of in an appropriate, legally compliant manner, irrespective of format.

The retention schedule to which this policy refers takes into account relevant requirements of the University's regulations and policies, as well as recommendations of the Joint Information Systems Committee (JISC) Retention Schedule and common practice within higher education.

## 3. Scope

The policies in this documentation set apply to all records the university handles whether or not they are owned by the University.

The policy is aimed at all staff. Unless otherwise stated, it is the responsibility of departments to retain the items listed in the schedules and to assign specific individuals to have responsibility for each category.

Lead to the development of documented procedures and processes to enable the University to comply with the policy.

## 4. Definition of a records retention schedule

The records retention schedule is a practical document that details the classes of records held by the University and metadata about them for the purposes of preventing premature destruction or unnecessary retention of records. It lists the length of time for which categories of records should be retained in order to meet compliance and business requirements. It specifies when records need to be destroyed and the person(s) responsible to ensure this.

It records:

- categories of records held
- the format in which the master record should ideally be retained;
- the event which triggers the retention period to begin
- a subsequent retention period for each category
- what to do with the record when the retention period expires
- the rationale for the retention
- additional context and examples

The retention schedule is owned by the Information Compliance team and will be made accessible to all staff via the Governance pages on the website.

## 5. Enforcement & review

The policy cannot be pro-actively enforced in the absence of an Electronic Documents and Records Management System, but the introduction of the Records Management Framework and Data Officer roles will provide support and guidance to staff in respect of managing records in their business areas.

The schedule should be updated by all departments on an ongoing basis. A review must be organised at least annually by the Data Officer. It must also be updated to reflect changes in legislation, regulation or audit requirements and/or university business practice. The schedule should be reviewed by the Information Compliance team.

Where a department requires a record for longer than the retention period specified in the retention guide, this should be notified to the Data Officer for review. Where appropriate, the Data Officer will liaise with the Information Compliance team.

## 6. Implementation

Responsibility for implementing the schedule will need to be assigned to appropriate members of staff within the faculties and departments holding the records. They should maintain a local record of when specific records meet their destruction/disposal date.

## 7. Storage and preservation

Documents need to be arranged systematically and labelled helpfully and consistently, so that it will be possible to locate them with ease and respond promptly to enquiries.

Paper Records should have a file cover labelled with a disposal date, so that it is easy to locate material due for destruction. In the case of electronic information, a logical hierarchical structure of folders, subfolders and metadata should be used to ensure that documentation can be readily identified for deletion.

Local storage for paper records should be secure and protect the records from water damage (from flooding, leaks, or sprinklers), fire damage, light damage, large fluctuations in temperature/humidity and pests.

Vital records (without which the department could not function) should be prioritised for protection. Appropriate measures must be enacted to ensure access to vital records is maintained for business continuity purposes.

Records held electronically must be held securely but remain accessible to appropriate members of staff. Business areas must review their data periodically (ideally every five years) and, if necessary, arrange for it to be converted to new file formats, particularly where retention is greater than seven years.

All critical, long-term electronic data needs to be held on a server, so that it will be adequately backed up and safeguarded from hardware failure.

## 8. Destruction

Before any corporate value records are destroyed the record owner must authorise the university's nominated party or parties responsible for destruction and record this decision.

All records must be securely disposed of in accordance with the University's legal compliance obligations, but particular care must be taken with records marked as confidential or containing personal data.

An accurate audit trail of records destroyed must be maintained by the University's nominated party or parties responsible for the destruction of records.

Where a record is subject to pending investigation or litigation it must not be destroyed. The closure of the investigation or litigation will then be the 'last action' from which retention is calculated.

## 9. Relevant legislation

The University is required to comply with a variety of legislation affecting the use and retention of its records, including, but not limited to the following:

- Civil Evidence Act 1995
- Data Protection Act 1998
- General Data Protection Regulation
- Education Act 1994
- Electronic Communications Act 2000<sup>1</sup>

---

<sup>1</sup> Confirms legal basis of electronic signatures  
Records Retention and Disposal Policy

- Equality Act 2010
- Freedom of Information Act 2000
- Health & Safety at Work Act 1974
- Limitation Act 1980
- Public Services Contract Regulations 1993
- Taxes Management Act 1970
- Unfair Contract Terms Act 1977
- Value Added Tax Act 1994

## **10. References to other policies**

- Records Management Policy
- Data Handling Standards Policy
- Information Security Policy

## **11. Document approval**

- Approved by: Information Management and Security Steering Committee
- Approved Date: 21 May 2018
- Review Date: September 2019
- Reviewer:

## **12. Document history**

25th April 2018 – Draft 0.1 Fraser Marshall  
21 May 2018 – v0.2 approved by IMSSC

## Appendix 1 – Examples of Records

The following is a list of a few examples of records that are held by the University taken from the current Retention Guide. The purpose is to show the kinds of information deemed to form a record.

- Information documenting the handling of applications for admission: successful applications.
- Information documenting the handling of applications for admission: unsuccessful applications.
- Final versions of publications and presentations made to disseminate research results (NOT interim or final research reports).
- Information documenting marks/grades given to submitted/completed summative assessments and, where appropriate, awards and classifications.
- Information documenting feedback on academic progress, and general academic guidance and support, given to individual taught students.
- Records documenting the administration of academic programmes.
- Master copies of procedures relating to academic award administration.
- Master copies of procedures relating to corporate planning and performance management.
- Information documenting the development of the institution's strategic plan: key records.
- Information documenting security breaches or incidents, and action taken.
- Information documenting leasing-out arrangements for properties.
- Information documenting the conduct and outcomes of space audits.