Scope: Data Protection	Effective Date: January 2023	Responsible Dept: Governance & Compliance	Equality Analysis Undertaken:
Last updated by/date: Information Governance Assistant; December 2022	Next review date: January 2024	Approved by: Executive Board 17/01/23	Policy ref:

Data Retention and Erasure Policy

1 Introduction

The aim of this policy is to ensure that the retention and disposal of records is consistently managed across all departments and schools. According to the storage limitation principles set out in the UK General Data Protection Regulation (UK GDPR):

- personal data must only be retained for as long as it is needed;
- the period of retention should depend on the agreed purposes for holding the data;
- Retention Schedules should be prepared and maintained for all records;
- periodic reviews of data held should be performed and records should be erased, archived, or in some cases anonymised, where necessary;
- it should be noted that data subjects have a right to access or request erasure of their personal data;
- personal data can be retained for longer if kept for public interest archiving, scientific or historical research, or statistical purposes.

2 Retention Schedules

It is important that each directorate and school prepares and maintains a Local Retention Schedule to ensure that records are only retained for as long as they are needed and that they are efficiently disposed of thereafter.

Each department should decide upon the time limits for retaining records and clearly record these decisions via their Local Retention Schedule. All Retention Schedules should be stored on the Records Retention page of the University's Staff Intranet and reviewed every six months.

As the UK GDPR does not set specific time limits for different types of data, in order to support consistency York St John University uses the recommendations and templates provided by JISC Records Retention Management. Each Local Retention Schedule should include the following:

- categories of records held by the University;
- descriptions of each record;
- the primary area of responsibility;
- the local record holder;
- retention period & disposal;
- the master record holder;
- format of record held whilst current;
- format of record held whilst archived.

The University's template for Local Retention Schedules can be downloaded from the Staff Intranet.

The recommended periods of retention for higher and further education institutions can be found at https://www.jisc.ac.uk/guides/records-retention-management.

3 Why Are Retention Schedules Required?

Retention Schedules should be prepared and maintained in order to:

- provide a clearly defined system for the retention and disposal of records;
- prevent records from being prematurely destroyed;
- ensure information is not kept unnecessarily;
- help to save space, time and money;
- promote sustainability.

The Data Protection Act 2018 requires that personal data be protected from unauthorised destruction and retained for no longer than is necessary.

The Freedom of Information Act 2000 requires that the disposal of records is undertaken in accordance with clearly established policies which have been formally adopted and enforced by the authorised staff. It is an offence to destroy any document held by a public body to prevent disclosure of information. Retention Schedules assist in defining clear procedures for retaining and discarding records legitimately.

4 Implementation

For each department and school, an appropriate member of staff should be assigned to ensure that local retention schedules are created and maintained. A system should be implemented to ensure that departments are alerted to forthcoming retention deadlines and that destruction or anonymisation of data is actioned in a timely manner.

5 Storage and Preservation

Both digital and paper documents should be arranged systematically and labelled clearly and consistently to enable ease of location. Where possible, disposal dates should be included within the documents.

If paper documents need to be retained, they should be clearly documented in retention schedules and stored systematically in a safe and secure environment. Local storage for paper records should protect the records from:

- Water, fire and light damage
- Temperature/environmental fluctuations
- Pests

It is essential that regular reviews of records take place to ensure that data is always accessible, usable and has not become locked in obsolete technology. If data is no longer of any use, it should be immediately and securely disposed of.

6 Disposal

6.1 Routine Disposal

Some data can be disposed of frequently and departments and schools should clearly record such requirements on their local retention schedule. A system of routine disposal should be agreed on and implemented accordingly.

6.2 Secure Disposal

Sensitive data should be disposed of securely and in accordance with the University's confidential waste processes. Support with the secure destruction of digital data and hardware should be obtained from the Governance and Compliance team and, where necessary, the ICT department.

6.3 Authorisation and Recording of Disposal

Each department and school should assign an appropriate member of staff to oversee the disposal of data. Disposals of sensitive data, as well as any large-scale disposals, should be authorised by the appropriate member of staff and a record of such disposals should be added to the relevant Retention Schedule.

6.4 Legal Hold

If data needs to be retained due to pending litigation or investigation, or if the data is known to be subject to a Freedom of Information or Subject Access Request, the disposal of the data should be delayed until legal procedures have been concluded and/or the data has been disclosed as part of the data request.

7 Data Erasure Requests

The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in the following circumstances:

- the personal data is no longer necessary for the purpose which the University originally collected or processed it for;
- the University is relying on consent as its lawful basis for holding the data, and the individual withdraws their consent;
- the University is relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the University is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the University has processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- the University has to do it to comply with a legal obligation; or
- the University has processed the personal data to offer information services to a child.

Individuals can make a request for erasure verbally or in writing. Requests received by the University should be immediately forwarded to the Information Governance Officer or emailed to foi@yorksj.ac.uk. The University has one calendar month to respond to a data erasure request.

When a request is received, it may be necessary for the University to seek proof of identification from the sender. The University should not comply with the request until it is satisfied that the sender is who they say they are and should close the request if proof of identity has not been provided within one month. Copies of the following forms of ID are acceptable:

- Birth Certificate
- Driving Licence
- Passport
- Proof of Age Card
- National Identity Card
- Medical Card
- Benefits letters

Once the data has been removed from all systems, the sender should be informed and all related emails or copies of communications removed thereafter. It is acceptable to keep only minimal information relating to the sender within the University's data erasure request log but this should be removed as soon as it is no longer required.