



Data Retention Policy

Document Control	
Document Owner	Director of Operations
Version	1.2
Approved By	RSN Council
Date	20 th July 2022
Effective Date	1 st August 2022
Amended By	Policy Working Group
Amendment Date	20 th July 2022
Amendments	Extraction of procedure and schedule Archivists Role Change of effective date
Formal Review Date	1 st August 2024

This policy reflects legislation and official guidance at the time it was last reviewed. Any changes in legislation will take precedence over anything printed in this policy. Where other policies are referred to they can be viewed at the Policy Library

Data Retention Policy

1. Policy statement

The RSN has established this Data Retention, Archiving and Destruction Policy (the “Policy”) in order to set out the principles for retaining, reviewing and destroying data enabling a consistent approach throughout the organisation.

2. Policy Scope

This policy applies to all individuals doing work for the RSN at all levels and grades, including staff, Trustees, casual workers and agency staff, free-lance tutors and contractors. It does not include degree students who are covered by the policies of the presiding university. This policy represents the minimum standard expected from staff and others involved in the RSN. If applicable law requires a higher standard or additional requirements, then these must be adhered to.

3. Policy Coverage

This Policy covers all data retained or in the RSN’s possession (including data on own devices that relates specifically to the RSN business or clients or control in whatever medium such data is contained. This includes both paper documents and data contained in an electronically readable format (both hard and soft copies). For the purposes of this Policy, the medium which holds data will be referred to as “Document”.

Personally Identifiable Information (“Personal Data”) differs slightly from ordinary data and is subject to the General Data Protection Regulation (EU) 2016/679 (“GDPR”). Other national laws in connection with data protection may also apply. Any Document containing Personal Data shall fall under that section of this Policy.

4. Objectives

The RSN is bound by various obligations with regard to the data that we retain or is in our possession or control. These obligations include how long we may retain data and when and how we can destroy it. The obligations may arise from local laws or regulations or from contracts or other agreements that we have made between members of our workforce, customers and our suppliers.

5. Retention

Retention is defined as the maintenance of documents in a production or live environment which can be accessed by an authorised user in the ordinary course of business.

RSN's Documents must be stored in a safe, secure and accessible manner. Any Documents that are essential to our business operations during an emergency must be duplicated and/or backed up at least once per week.

6. Archiving

Archiving means secured storage of Documents such that documents are rendered inaccessible by authorised users in the ordinary course of business, but which can be retrieved by an administrator designated by the head of department for the Documents in question.

Electronic records shall be archived in accordance with the RSN's Information Security Policy for access controls and in a format which is appropriate to secure confidentiality, integrity and accessibility of the Documents.

7. Organisational archive

In order to maintain a history of the organisation it is important that a variety of documents are kept in perpetuity and not destroyed after their 'working life'. Records that are identified for indefinite retention must be retained and appraised by The Chief Executive (in her role as archivist) or any appointed archivist.

8. Destruction

Destruction means physical or technical destruction sufficient to render the information contained in the document irretrievable in line with industry standard.

The RSN is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction.

9. Personal data

The GDPR imposes obligations on the RSN as a data controller as well as a data processor. Both must process personal data in a fair manner which notifies data subjects of the purpose of data processing and to retain the data for no longer than is necessary

to achieve the purpose that it was collected for. Further retention of the personal data will only be lawful when it is compatible with the purpose for which it was originally collected.