Data Retention Procedure

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

This procedure 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 on the Policy Library.

Data Retention Policy - Procedure

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. Who is covered by the policy

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. What is covered by the policy

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. Procedure

4.1 The RSN may from time to time be involved in unpredicted events such as litigation or business disaster recoveries that require us to have access to the original Documents in order to protect the RSN's interests or those of the members of our workforce, customers and our suppliers. As a result, Documents may need to be

archived and stored for longer than the data may be needed for day to day operations and business processes.

4.2 When the Document Retention Period is over and we no longer need the Document, the RSN will destroy it in a proper manner.

4.3 The retention period of the different types of Documents shall be defined in Schedule 1 of the Data Protection Policy

4.4 After the retention period has expired and according to appropriate exceptions, certain Documents shall be archived in accordance with Appendix 1 and section 6 of this Policy until the Documents are destroyed in accordance with section 7.

4.5 To enforce retention in accordance with this Policy, each department is responsible for the Documents it creates, uses, stores, processes and destroys.

4.6 If any Document retained under this Policy is stored in an encrypted format, consideration must be taken for secure storage of the encryption keys. Encryption keys must be retained for as long as the data that the keys decrypt is retained.

4.7 Each member of our workforce shall be responsible for returning Documents in their possession or control to the RSN when they cease to be a member of our workforce. Final disposition of such Documents shall be determined by the member of our workforce's immediate supervisor in accordance with this Policy.

5. Archiving Procedure

5.1 Paper records shall be archived in secured storage onsite or secured in an offsite location, clearly labelled in archive boxes naming the department and a date to be destroyed. Inside the archive box should be a table of contents to enable the administrator to locate specific Documents. A copy of the table of contents shall be provided to the head of department at the time of archiving to ensure there is a suitable record kept with the relevant destruction dates noted.

5.2 The relevant archive period of a Document is specified in Appendix 1.After the archive period has expired, Documents shall be destroyed in accordance with section 8. For the purposes of enforcing archiving in accordance with this policy, each department is responsible for the Documents it creates, uses, stores, processes and destroys

5.3 Records with lasting historic interest and business value will be identified through a “Retention Schedule”

5.4 Records that are identified for indefinite retention must be retained by the Section Head. Following this they shall be appraised by the RSN Archivist and transferred to the RSN Archive.

5.5 These records will provide an enduring record of the conduct of RSN.

6. Destruction

6.1 All Documents that have met their required retention period or are no longer being used, or required by the business shall be destroyed in the following ways:

6.1.1 Non-confidential / Non-Sensitive Documents: Can be placed in normal waste or recycling;

6.1.2 Confidential / Sensitive Documents: Shredded, or placed in confidential waste bins for destruction;

6.1.3 Electronic equipment containing Documents: Can be provided to IT for secure wiping and disposal;

6.1.4 Destruction of electronic records should render them non-recoverable in line with industry standards.

7. Personal data

7.1 As part of the GDPR requirements individuals have the right to be informed how their data is processed and we are therefore obliged to provide individuals with information on our retention periods or criteria used to determine the retention periods.

7.2 Individuals have the right to have their personal data erased and no longer processed in the following circumstances:

7.3 Where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;

7.4 Where a data subject has withdrawn his or her consent or objects to the processing of their personal data (e.g. Marketing). For the avoidance of doubt where we are under a contractual or legal obligation to process the data subjects personal information or for the prevention or detection of crime this information shall be retained as specified in Appendix 1.

7.5 Where the processing of their personal data does not otherwise comply with the GDPR.

7.6 After the expiration of the applicable retention period personal data does not always have to be completely erased. It is sufficient to anonymise the data if the organisation deem it necessary. This may for example be achieved by:

7.6.1 erasure of the unique identifiers which allow the allocation of a data set to a unique person;

7.6.2 erasure of a single piece of information that identifies the data subject (whether alone or in combination with other pieces of information);

7.6.3 separation of personal data from non-identifying information; or

7.6.4 aggregation of personal data in a way that no allocation to any individual is possible.

7.6.5 In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

7.6.6 the pool of data has grown so much that personal identification is not possible based on the information retained; or

7.6.7 the identifying data has already been deleted.

7.6.8 In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of the processing. This means that the data shall be deleted or destroyed in accordance with the policy.