Information and Data Retention

Policy

Contents

[1. Policy Statement 3](#_Toc493574650)

[2. Scope 3](#_Toc493574651)

[3. Principles 4](#_Toc493574652)

[4. Responsibility 4](#_Toc493574653)

[5. Assurance 5](#_Toc493574654)

[6. Reviews 5](#_Toc493574655)

[7. Associated Documents and Policies 5](#_Toc493574656)

Information and Data Retention Policy

# Policy Statement

Information is a key resource for the organisation and must be successfully managed to ensure the efficient and effective delivery of service, and the continued confidence of our supporters.

The RNLI has a duty to comply with legal requirements and best practice guidelines in relation to the retention and secure disposal of both paper and electronically stored information.

The key objective of this Policy is to provide the organisation with a simple framework which will govern decisions on whether a particular piece of information should be retained or disposed of.

The Information Asset Register appended to the Information and Data Retention Procedures lists the different types of information held by the organisation and the retention periods that apply to each, as well as how each should be stored and disposed of.

The aims of the policy are to:

* Promote improved Records Management practices within the organisation
* Assist in the identification and management of information that attracts statutory or best practice retention periods
* Prevent the premature destruction of information that should be retained for a specified period to satisfy legal, evidential, financial and other requirements
* To ensure information is kept safe from loss, damage or tampering
* To ensure information is disposed of in a way which is auditable and meets all environmental and other requirements
* Assist in identifying information that should be preserved permanently as part of the Heritage Archives

This policy should be read in conjunction with the Information and Data Retention Procedures.

# Scope

This policy extends to all permanent and temporary employees, volunteers, contractors and others who may have access to, or reason to otherwise retain or dispose of information and data on behalf of the RNLI.

# Principles

* 1. Information is a key resource for the organisation and must be successfully managed to ensure the efficient and effective delivery of service, and the continued confidence of our supporters.
	2. In order to comply with the General Data Protection Regulation, personal data should be kept for no longer than is necessary for the purpose for which it was collected, at which point it should be securely disposed of. It is good practice for this principle to be extended to all information.
	3. Personal data should not be retained to be used for a new purpose that is incompatible with the purpose for which it was originally collected. In the event that there is a requirement for personal data to be retained for a new purpose advice should be sought from the Data Protection team.
	4. The primary drivers that inform decisions on retention are:
* Business need - as agreed by the Executive Team
* Legislative and regulatory requirements – for example compliance with the fifth data protection principle, *‘personal data shall be kept no longer than is necessary for the purpose you obtained it for’.*
* Heritage and Archives requirements or guidelines
	1. Information shall be kept securely. The level of security will depend upon the nature of the information held.
	2. Retention periods apply to all formats of information, e.g. paper, electronic, images, oral recordings etc. unless specifically stated otherwise.
	3. The organisation shall ensure secure and appropriate disposal of information.

# Responsibility

* 1. All individuals within scope are required to ensure they comply with this policy, the associated procedures, and relevant legislation, when undertaking their role.
	2. The Executive Team is responsible for ensuring knowledge and responsibility of information and data retention is embedded across the organisation.
	3. Line Managers are responsible for ensuring that this policy is applied within their own area.
	4. Prior to undertaking any work for, or on behalf of the RNLI, all volunteers must read the “*Guidance for Volunteers on Data Protection*”. If volunteers retain any information outlined in the Information Asset Register they must ensure that they follow the Information and Data Retention Procedures.
	5. Any queries on the application or interpretation of this policy and/or associated procedures must be discussed with the Legal team prior to any action being taken.
	6. The Legal team, within the Business Services and Support Department has the responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments or alterations to the policy and/or procedure can only be implemented following approval by the Legal team.

# Assurance

The Compliance Duty Holder (Anjie Rook, Director of Business Services and Support) needs to be assured that this policy is working:

1. It is doing what it is supposed to do on the ground

2. It is effective at delivering the organisational objectives.

This will be achieved by having:

* A Compliance Duty Holder in place to oversee the policy.
* A Data Governance Authority in place to oversee the management and compliance of the RNLI with the Policy.
* Regular audits and reports will be carried out by the Data Governance Working Group to assess compliance with policy.

# Reviews

Reviews of this policy will take place at least once a year. However more reviews may be triggered by any of the following items and assessed by the Data Governance Authority and the Compliance Duty Holder:

* Escalation of related strategic risks
* Significant ethical changes
* Legal, regulatory or operational changes
* External or internal incidents (e.g. data breach, negative publicity)
* New technology
* Financial changes
* Changes to governance.

# Associated Documents and Policies

* Information and Data Retention Procedures
* Appendix 1 – Information Asset Register
* Appendix 2 – Record Disposal Procedure
* Appendix 3 – Record Disposal Log
* Data Protection Procedure
* Information Management Policy
* IT Systems Policy
* Guidance for Volunteers on Data Protection