Policy Title
Data Protection Policy

Policy Owner	Owning Dept
Nicky Nelson	Legal

Last Updated	Next Review Date
01/10/2022	01/10/2025

Reason for Policy

To define the RNLI's approach to the processing of personal data and the standards it will adopt to meet its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

Objective of Policy

To set out minimum standards and best practice requirements adopted by the RNLI to ensure that it meets the obligations of the relevant legislation, the privacy expectations of the persons whose personal data it processes, and outline the steps it will take to ensure that it meets those standards.

Applicability

This policy applies to all permanent and temporary employees, volunteers and contractors who have access to, or reason to otherwise process personal data on behalf of the RNLI.

Third parties or contractors that the RNLI engages will only process personal information on our instructions or with our agreement, and where they do so they have agreed to treat the information confidentially and to keep it secure.

It applies across all RNLI locations in the United Kingdom, Republic of Ireland, Channel Islands and the Isle of Man and to the personal data of any individual regardless of where in the world they are located.

This policy also applies to all processing undertaken by any wholly owned subsidiary company of the RNLI.

Policy

1. RNLI Data Protection Roles and Responsibilities

Roles

DPO - Data Protection Officer.

The DPO is responsible for advising the organisation, its staff and volunteers of their data protection responsibilities and ensuring the organisation manages personal data lawfully. The DPO reports directly to the Executive Team on RNLI's data protection risk and compliance status.

Accountable Data Executive

The Accountable Data Executive (at Director level) is ultimately accountable for the legal, ethical and effective use of defined data entities which are assigned to them. In addition, they are accountable for all processes consuming data within their business stream.

Data Owner

Appointed by the Accountable Data Executive, the Data Owner has delegated accountability for governing the collection, use and management of data within a defined data set or within a specific process.

Data Manager

The Data Manager is appointed by, supports and deputises for the Data Owner. They are responsible for the day-to-day operation and management of processes involving (creating, updating, utilising, removing, etc.) data.

Data Steward

The Data Steward supports the understanding, embedding and operation of the Data Governance principles and other initiatives within the department they represent.

Responsibilities

Data Protection legislation places a legal requirement on the RNLI to put in place measures to implement the data protection principles effectively and safeguard individual rights.

This means the RNLI must integrate data protection into all processing activities and business practices, from the design stage right through the data lifecycle - 'data protection by design and by default'.

All line managers are required to ensure that the processing undertaken by individuals reporting to them complies with the requirements of this policy and the relevant legislation.

Everyone who processes personal data on behalf of the RNLI is responsible for ensuring they understand their responsibilities and comply with the requirements of this policy.

Failure to comply with the requirements of this policy or the relevant legislation constitutes a serious breach of the applicable Code of Conduct and may result in action, which could include dismissal, being taken under the Disciplinary Procedure Policy or Volunteer Problem Solving Policy as appropriate.

2. Information Covered by Data Protection Legislation

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

Some personal data is categorised and needing a higher level of protection. This is known as sensitive or special category personal data and includes information relating to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convections and offences)

3. Principles relating to the processing of personal data

All processing of personal data undertaken by the RNLI must be in compliance with the 6 principles set out below. Data should be:

(a) be processed **fairly, transparently** and under one of the six legal bases,

- Consent
- Contract
- Legal Obligation
- Vital Interest
- Public Interest
- Legitimate Interest

(b) only be **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes;

(c) be **limited** to ensure that

- only enough personal information adequate for the purpose and
- only relevant personal information and
- only personal information necessary to the purpose is processed.

(d) **accuracy** - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate. Any inaccuracies found must be rectified without delay;

(e) **storage limitation** - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

(f) **integrity and confidentiality** - processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. The legal basis for processing of personal data

All processing of personal data undertaken by the RNLI must be undertaken under one of the six specified legal bases as set out below. The particular legal basis being used must be identified and recorded prior to any processing being undertaken.

i. **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes

ii. **Contract** - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

iii. **Legal obligation** - processing is necessary for compliance with a legal obligation to which the controller is subject;

iv. **Vital interests** - processing is necessary in order to protect the vital interests of the data subject or of another person;

v. **Public interest** - processing is necessary for the performance of a task carried out in the public interest;

vi. **Legitimate interests** - processing is necessary for the purposes of the legitimate interests pursued by the controller. Such interests must not be overridden by the interests or fundamental rights of the data subject in particular where the data subject is a child.

5. Processing special categories of personal data

The RNLI processes special category data under the following legal bases:

- The data subject has given explicit consent to the processing the information for one or more specified purposes.
- In the field of employment and social security and social protection law
- Necessary to protect the vital interests of the data subject
- For defence of legal claims
- For reasons of substantial public interest
- Health or social care (with a basis in law)
- Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

The RNLI processes criminal data in the following key areas:

- To assess and individual's suitability for employment
- To assess an individual's suitability as a volunteer
- To process insurance documentation

6. Respecting the rights of the data subject

The rights granted to data subjects are:

- **Right of access:** The data subject has the right to access of the personal data being processed. Access must be provided free of charge.
- **Right to rectification:** inaccurate data must be corrected without delay and incomplete data completed upon request.
- **Right to erasure:** also known as the 'right to be forgotten' this provides that under certain circumstances the data subject can oblige the data controller to erase personal data relating to them without undue delay.
- **Right to restrict processing**: under certain circumstances the data subject can object to processing other than storage of their personal data.
- **Right to data portability**: this entitles the data subject to a copy of their personal data in a structured and commonly-used machine readable format and allows them to require it to be transmitted to another data controller.
- **Right to object to processing**: a data subject may object to processing including the profiling of the data subject, which is undertaken under the public interests or legitimate interests bases, and can also object to the processing of their data for direct marketing purposes.
- **Right not to be subject to automated individual decision-making**: data subjects can object to 'automated processing' (which includes profiling) if that processing results in decisions which have a legal effect concerning him or her (or similarly significantly affects them) being made solely on the basis of that processing.
- **The Right to be informed.** All individuals whose personal data will be processed by the RNLI will be presented with a Fair Processing Notice which signposts them to the RNLI Privacy Notice.

The RNLI is legally obliged to complete all data subject rights request within one month. All requests received must be forwarded to Data_Protection@rnli.org.uk without delay.

7. Personal data breaches

Everyone who processes personal data on behalf of the RNLI shall ensure they take all appropriate and reasonable precautions to prevent a personal data breach occurring. In the event they become aware of such a breach they will report the matter immediately to the Data Protection team Data_Protection@rnli.org.uk

A personal data breach means a lapse in security which has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The following are examples of data breaches (this list is by no means exhaustive):

- Loss or theft of RNLI device containing personal information
- Personal data sent to an incorrect email recipient
- Documents containing personal information misplaced, lost or stolen
- RNLI data systems compromised or "hacked"
- Incorrect details added to a personal file on a system such as CRM, HR or financial record

- Lost or incorrectly addressed mail
- Personal information inappropriately filed on shared drive
- Personal information is shared without appropriate legal basis

The Data Protection Officer is legaly obliged to notify any reportable personal data breach to the Information Commissioner's Office (ICO) within 72 hours. Therefore all personal data breaches and near misses must be reported **immediately** to Data_protection@rnli.org.uk. to enable the DPO to assess the breach to determine whether or not it is reportable.

8. Data Protection Impact Assessments

Data Protection by Design and Default requires the RNLI to integrate protection principles into all processing activities and business practices, from the design stage right through the lifecycle.

Therefore, when considering a new process, procedure, product or project which may include using personal data, the Data Manager shall contact Data_Protection@rnli.org.uk with a brief synopsis of the proposal at the earliest stages of planning. The Data Protection team will work with the Data Manager or relevant team leader to undertake a Data Protection Impact Assessment (DPIA) screening exercise to ascertain whether or not a full DPIA is required.

No new process, procedure, product or project using personal data shall be implemented until a full DPIA has been completed and signed off by the DPO.

9. Transferring Personal Data outside the RNLI

The RNLI may engage with third parties to carry out work which will require personal data to be transferred to those third party Data Processors (e.g. sending a list of supporters' names and addresses to a mailing house to fulfil a marketing campaign).

The RNLI will only use Data Processors that are able to;

- provide guarantees, that they have appropriate organisational and technical measures in place to ensure the data is processed in compliance with legislation and
- who have signed a binding contract which specifies the purpose for which the personal data is transferred, restricts the processing to that purpose, specifies the duration of the contract and sets out how the data will be dealt with at the end of the contract.

RNLI standard clauses must be incorporated into every contract appointing a data processor. Support can be provided by the Procurement, Legal and Data Protection Teams.

Transfers of Personal Data Overseas

Before any personal data can be transferred overseas this processing must be signed off by the DPO via a completed DPIA and an appropriate contract must be in place.

10. Data Protection training

All RNLI staff must complete the mandatory Data Protection Training as part of their induction. All employees must complete the refresher training annually.

Additional training data protection training may be provided if relevant to a specific roles.

11. Record keeping

The RNLI shall ensure that sufficient records are kept of the organisation's processing activities to include:

- A Register of Processing Activity (ROPA) detailing the personal data assets processed, the nature of the processing, the systems used, the legal basis, the time for which the data will be retained and how it will be disposed of.
- A register of Data Protection Impact Assessments undertaken which includes screening only results. .
- A register of Privacy Policies, procedures and statements
- A Personal Data Breach log
- A register of all data subject rights requests received and completed.
- A register of all training required, completed and outstanding.
- Where consent is the legal basis for processing personal data, process managers should ensure appropriate records and documentation is retained to evidence consent.

12. Monitoring and Assurance

Compliance with this policy will be monitored by the DPO and responsible teams reporting into the Executive Team, Audit & Risk Committee and the Trustee Board.

Definitions

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier;

'processing' means any operation which is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, use, disclosure, erasure or destruction;

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'processor' means a person, public authority, agency or other body which processes personal data on behalf of the controller;

'recipient' means a person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;

'near miss' any incident that had the potential to cause a data breach even though it might not have done so.

'privacy by design and default' to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.

Relevant Legislation

UK Legislation:	The Data Protection Act 2018, (**DPA**)
	UKGDPR
Irish legislation:	The Data Protection Acts 2018 (**IDPA**)
Jersey legislation	The Data Protection (Jersey) Law 2018 (**JDPA**)
Guernsey legislation:	Data Protection (Bailiwick of Guernsey) Law 2017 (**GDPA)**
Isle of Man legislation	Data Protection Act 2018 (**IOMDPA)**
EU Legislation:	The General Data Protection Regulation (GDPR) The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

Related Policies, Procedures & Guidance

- RNLI Retention Policy
- Information Security Policy
- Acceptable Use Policy
- Data Governance Policy
- RNLI Privacy Policy
- Data Subject Request Procedures
- Data Protection Impact Assessment Procedures
- Due Diligence and Networking Research data collection and retention procedures