Policy Title	Version Number
Information Security Policy	**V2.4**

Policy Owner	Policy Author
Head of ITS Services & Security	**Information Security Manager**

Last Reviewed	Next Review Date
1st February 2023	**15th February 2025**

Reason for Policy

Information systems are key to the RNLIs lifesaving operations, fundraising activities and our vision to save everyone. It is therefore essential that everyone who uses information and/or systems understand how they can safeguard the confidentiality, integrity and availability of any information they may collect store or access. Any risk to our information or systems has the potential to cause reputational damage as well as financial and regulatory impacts.

Objective of Policy

To provide a framework for managing information security throughout the Institution and ensure we all preserve the key principles of information security in order to protect the RNLIs reputation:

Confidentiality:	Protecting information from unauthorised access or disclosure.
Integrity:	Preserving accuracy and authenticity of information without unauthorised or accidental modification
Availability:	Ensuring information is accessible and useable where and when required including appropriate disposal when no longer of purpose or value.

Applicability

This policy always applies to:

- Anyone with access to RNLI systems, including staff, volunteers, contractors, suppliers or partners.
- All data collection, processing, transferring, retention and disposal, electronically or physically.
- All systems connected to the RNLI computing or telephone networks.
- All computer equipment purchased by the RNLI and personal mobile devices being used to access RNLI systems and/or information.
- All third parties that provide a service to the RNLI via access to systems or information or those who process any information on behalf of the RNLI.
- All RNLI Cloud environments.

Policy

1. Information Security Principles

- It is everyone's responsibility to ensure that any mandated training aligned to cyber threats (such as Phishing), information (GDPR etc) or technology, is completed in a timely manner.
- All RNLI information must be protected in line with its relevant classification, internal policies and all relevant legal and regulatory requirements.
- All RNLI information must be classified in line with the RNLI Data Classification guidelines and protected or handled appropriately.

- ❖ Every RNLI computing asset has a nominated owner who is solely responsible for the appropriate use of information on it and ensuring appropriate security measures remain in place to protect the asset.
- ❖ Encryption of information and computing assets must be applied at all times by either users (portable media devices such as USBs / Portable Hard Drives, etc) or the IT department (devices, databases, etc). Security settings must never be tampered with or turned off/disabled.
- ❖ Any faulty, damaged, lost or stolen devices (computers, tablets, phones, and portable media) must be reported immediately to the IT Service Desk where a replacement can be arranged, if necessary.

Managers must:

- ➢ Ensure that they and all existing and any new team members are aware of all relevant RNLI policies that relate to their role when using RNLI computers, computing resources, information and physical (paper) copies of any information.
- ➢ Ensure that they and all team members complete all mandatory training in a timely manner and if this is reported as overdue that time is given immediately to cover this as soon as practically possible.
- ➢ Ensure that they notify HR of any starters, movers or leavers in their team in a timely manner. Any leavers accounts must be deactivated on their last working day.

1. People:

Users must: *(Including managers)*

- ➢ Ensure that any details (e.g ID / Password / PIN) or account access relating to information or systems is not shared with anyone.
- ➢ Ensure they protect any computing devices and report to the IT Service Desk immediately if it becomes faulty, damaged, lost or stolen.
- ➢ Seek advice from infosec@rnli.org.uk or the IT Service Desk if you are unsure about any aspect of Information Security.
- ➢ Report any suspicious emails or activities immediately using the Phish Alert Button or to the IT Service Desk as soon as practically possible.
- ➢ Change your password if you have any suspicion that it may have been compromised.
- ➢ Report any actual or suspected loss of a RNLI device or information to the IT Service Desk.
- ➢ Ensure that any personal devices used to access RNLI systems or information are protected and secure and RNLI access is not shared with anyone else.
- ➢ Keep all software on personal devices up to date.
- ➢ Be aware of risks when using public Wi-Fi or public/shared computers and ensure you take appropriate action to securely access RNLI resources.
- ➢ Ensure that any paper-based information is securely locked away when not in use.
- ➢ Ensure your password/passphrase is strong and long and unique to your RNLI account. Never share your password with anyone as you are accountable for actions taken from your account.
- ➢ Advise when they are travelling abroad and will still be accessing their RNLI account, by emailing infosec@rnli.org.uk with details of the country/region and dates of travel. This will help us to identify valid access should your account be flagged as 'at risk' due to the location of access.
- ➢ Ensure your identity badge / card is visible whilst present in RNLI premises. This also applies to anyone accompanying a visitor and their temporary RNLI ID.
- ➢ Ensure that your computer connects to the RNLI VPN (Virtual Private Network) when working from home or remotely.

Privileged Users Must: (Access to systems that are above everyday user access)

- ➢ Request relevant access using the IT Self Service ticket, 'Privileged Access Request' in all

instances. Relevant approval must be granted before access can be reviewed and necessary privileges activated. This process is managed by the InfoSec Team, if there are any queries.

- Ensure that they do not access any email account or the internet using their privileged role.
- Never make any changes to IT Infrastructure, Network, Systems or security settings without relevant governance approval.
- Never take any action that will knowingly introduce vulnerabilities to any IT Infrastructure, Networks or systems.
- Ensure that only use this role for the time and task intended.
- Never share any login credentials with anyone.
- Report any suspicious activity or findings immediately to their manager and/or the InfoSec Team to ensure we maintain a secure technology environment.
- Never abuse this privilege under any circumstances.

2. Access to Information: *(All/Everyone)*

- All access to information outside of your normal role requirements must be approved by the information owner. Please refer to ……. For further assistance with this.
- Where you have access to information which relates to a previous role and is no longer part of your current duties, please report this to the data_gov@rnli.org.uk.
- If you can access information that you believe should not be viewable to you, report this immediately to the IT Service Desk for access to be reviewed by the information owner.
- Any physical information must be handled in line with its classification and stored securely.
- Physical copies of any 'Protected' or 'Confidential' information must only be discarded in confidential waste bins provided by the RNLI or shredded (Din4 or above for GDPR).
- Any external contractor, sub-contractor or supplier that requires access to RNLI information systems must be assigned individually identifiable user accounts only after a Privileged Access Request ticket has been authorised. (Located on IT Self Service)

3. Technology:

Users must: (Including Managers)

- Never install their own software/technology or that of a third party, without prior approval from the IT Department and necessary governance board. This could put the RNLI network at risk and may not be supported securely.
- Ensure that electronic information is always protected in line with the relevant classification and handling requirements. Refer to Data Governance Policy.
- Ensure that when travelling abroad, you check for any technology requirements or constraints for the country of destination when taking a RNLI device with you. https://www.gov.uk/foreign-travel-advice
- Ensure that they follow the Information Security Questionnaire (ISQ) process for any third-party service or access to information or the RNLI network that may be required prior to onboarding any supplier or third-party software. (Project and BAU related activities.)

Technical teams must:

- Ensure that password standards for users and privileged users are always implemented and adhered to.
- Ensure all endpoints (Technology, Devices, Networks, Servers) are regularly patched and kept up to date. Patches must be deployed within 14 days. (Ref: Cyber Essentials)
- Ensure any threat to technologies resulting in an incident are reported immediately, following either, the IT Incident Management Process or, Cyber Security Incident Response Plan only.
- Ensure any encryption keys are kept safe, secure and effectively managed. Any loss or compromise of these must be reported immediately with appropriate action being taken.
- Ensure all appropriate backups are scheduled and checked for successful completions with tests conducted periodically to ensure collection and restores are also successful.

- Ensure Disaster Recovery (DR) plans are documented, tested, amended/updated regularly.
- Promptly take action to report or uninstall software that is not licence compliant.
- Never install any software that is not approved by governance boards/teams or properly licenced.
- Ensure RNLI networks are designed and configured to high levels of performance, availability and reliability as appropriate for RNLI business needs, whilst providing a high level of control over access to the network.
- Ensure RNLI networks are segregated into separate VLANs (virtual local area networks) with routing and access controls operating between these in order to prevent unauthorised access and unnecessary traffic flows between them.
- Ensure any physical access to server rooms, networking and communications facilities are protected against unauthorised access, accidental damage, theft, tampering or any other malicious acts. Access (entry and exit information) must be recorded.
- Ensure all changes to infrastructure or network components are subject to the established change management process, where applicable. e.g., Production/Live environments.
- Ensure that robust controls are in place and managed effectively where gateways that link the RNLI network to the internet are protected against the risks of hacking, denial of service attacks, malware infection and unauthorised access to systems and information. Suitable controls must be applied to both incoming and outgoing traffic.
- Ensure that any changes to current information systems, applications, or networks that fundamentally alter the functionality or topography must follow the IT Change Management process.
- Security testing will be conducted at various stages of a project delivery, as well as regular testing throughout the natural life of a solution and following any significant change in line with the penetration testing policy.
- Ensure that any scanning or printing devices with scan to email capabilities are only enabled to scan to RNLI email addresses.
- Ensure any external contractor, sub-contractor or supplier that has authorised access via a defined user role or privileged access ticket is assigned an individually identifiable user account.

4. Devices:

Users Must: (Includes Managers)

- Always request technical (hardware) devices for RNLI use within their role via IT Self Services. Any other devices that are not approved may be blocked from accessing the RNLI network.
- Never tamper with or make any changes to the set up or security of any device entrusted to them.
- Ensure that all devices no longer required or, deemed fit for purpose, is returned to the IT Service Desk promptly.
- Ensure that any portable media devices, such as USBs & portable hard drives, are approved for business use, encrypted and have a strong password. That only RNLI approved devices are used and that access to the content on these are only to authorised personnel.
- Never plug any portable device into the RNLI network or computers if you are unsure where it has come from or what is held on it. Always, check with IT Service Desk first to run a physical check on it.
- Always ensure that any devices entrusted to them are protected from threats (left unattended and in sight in a vehicle, etc) and any environment hazards such as rain, spillages etc.

Technical Teams Must:

- Ensure any device connected to the RNLI network is managed effectively and does not allow to cause harm through unsupported operating systems, lack of control over secure

handling of information, etc. Any devices deemed non-compliant must be blocked or disconnected immediately.

- Recall all devices that are end of life and pose a security risk to the RNLI network.
- Disconnect any device from the RNLI immediately if it is identified as a security risk, until further investigations and/or actions taken, deem it to be safe.
- Ensure that any devices that are end of life or no longer fit for purpose are disposed of securely in line with internal processes.

5. Responsibilities:

Who:	What:
Data Protection Officer /Team	Accountability over all RNLI personal data to ensure that we comply with Regulatory requirements and Data Subject Rights.
Data Governance Team	Responsibility to assure compliance of users to the Data and Information Governance policy - to reduce and mitigate the risk of data loss or compromise.
Information Security Team	Responsibility to ensure that digital and physical controls are in place to reduce/mitigate risks to information and systems.
Architecture Board IT Change Board	Oversight of information security to new and current technology infrastructure ensuring that security by default and/or design is identified and implemented from the outset. Monitor, manage and approve any changes to RNLI technical infrastructure.
Information Owners System Owners	Responsibility to protect the information / systems they own by ensuring that access is only granted where appropriate to protect all information held and ensure unauthorised / inappropriate access is not granted.
IT Teams	Responsibility to ensure that necessary security controls are effective and working to safeguard systems and devices. Ensure preventative/detective controls are in place and any associated alerts are investigated to mitigate cyber risks.
Data Stewards	Provide support and assistance to their respective colleague's, promoting good information governance practices.
Users/Managers *(Everyone)*	Responsible for protecting the information that they access or process and use RNLI computing equipment responsibly. To report anything suspicious for computing or access to information to the IT Service Desk / InfoSec@rnli.org.uk. To complete all mandatory training in a timely manner.

6. Compliance:

Exceptions & Exclusions:

Any exception or exclusions to this policy must be raised following the Information Security Waiver Process. A Security Waiver ticket is available on IT Self Services, which must be completed for a decision to be made and any acceptable action taken, prior to any alternative ways of working taking place. Proceeding with alternative ways of working without approval, could result in disciplinary action.

Consequences:

Adherence to this policy reduces the risks associated with an information security incident that could result in;

- Unauthorised access to or disclosure of information or computer systems,
- Inaccuracy, incompleteness or invalidity of information or computer systems,
- Inaccessibility or non-availability of information or computer systems.

Such incidents would impact the RNLI through reputational damage, loss of goodwill from our supporters, legal proceeding, and fines from Regulatory bodies and would significantly jeopardise delivery of our strategic organisational objectives.

Information systems can be monitored and in the event of a security incident, systems may be shut down or seized without notice, for further inspection.

Failure to adhere to this RNLI policy will result in disciplinary action being taken.

Policy Audit:
This policy may be subject to Internal / External Audit and external regulatory review as appropriate.

External Reference Documents
Data Protection Act (DPA) 2018 **General Data Protection Regulation (GDPR) 2018** **Computer Misuse Act 1990** **EU Privacy and Electronic Communications Regulation (PECR) 2016** **Network and Information Systems Regulations 2018 (NIS Regulations)** **Telecommunications Security Act 2021** **Human Rights Act 1998** **NCSC Charities Guidance**

Related RNLI Policies, Procedures & Guidance (Available on Compass)
Acceptable Use Policy **Disciplinary Policy** **Data Governance Policy** **Mobile Device Policy** **RNLI Data Classification Levels** **Data and Information Governance Policy** **Social Media Policy**

Related RNLI Forms & Instructions (Available on Compass)
Information Security Waiver - Process and Form **Information Security Questionnaire (ISQ)** (Ticket in IT Self Services) **Information Asset Register**