Policy Title	Version Number
Acceptable Use Policy	**V3.0**

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

Last Review Date	Next Review Date
8th November 2022	**7th November 2023**

Reason for Policy

To promote a secure way of working in order to protect our people, processes, information and technologies deployed and utilised throughout the institution. It also provides clarity on the behaviours expected and required by all RNLI staff, volunteers, contractors and third parties.

Objective of Policy

To ensure that everyone is aware of their responsibilities with respect to the appropriate use of all RNLI Information Technology resources. Understanding of what is expected will help us all to protect ourselves, our colleagues and RNLI equipment, information and our 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 applies at all times to:

All RNLI representatives (staff and volunteers), contractors/consultants and third parties, regardless of geographical location.

- All RNLI equipment and information (printed or electronic, information systems, software, hardware, networks and applications).
- All channels of communication, including voice – telephony, social media, video, email, instant messaging, fax/printers, internet and intranet.
- Any employee, contractor, or volunteer accessing any RNLI information systems, applications or devices.
- Any third parties who access, host, process or support RNLI information, systems, or services.

Policy

1. Acceptable Use Principles

Users must:

2. Agree to always comply with this policy and raise any queries or concerns with their manager. Managers can then contact infosec@rnli.org.uk for security compliance or People Admin for any personnel queries.

2.1 Understand that breaching this policy could result in disciplinary procedures.

2.2 Be responsible for their own actions when using RNLI information and/or technologies to help maintain security, whilst also respecting colleagues, contractors or third parties when using these.

2.3 Always use any information, systems and/or equipment in line with RNLI Information Security Policy and all other relevant internal policies and laws. E.g., Data Protection, Computers Misuse Act.

2.4 Immediately report any breaches of this policy to their line manager and the Information Security Team

2.5 Never undertake any illegal activity, or any activity that would be harmful to the RNLIs reputation or jeopardise anyone's data that is held on RNLI technologies.

2.6 Understand that both business and personal use of RNLI systems or devices will be monitored as appropriate.

2.7 Never use a RNLI device or systems inappropriately that could be associated with malicious, harassing, abusive or threatening communications, visiting inappropriate websites that are not in line with your role or inciting hate, bullying and harassment, discriminatory behaviour or defaming another person or organisation.

2.8 The RNLI's approved cloud-based file storage service is Microsoft (OneDrive, Teams, and SharePoint). The use of any other cloud-based file service for storing RNLI files is not permitted without a formally approved Security Waiver.

2.9 RNLI telephony services are provided for you to conduct your daily duties. These services are also available for occasional personal use where necessary.

2.10 Ensure that all computing and telephony equipment is returned to your manager or the IT Service Desk when leaving the RNLI.

2.11 Understand that anyone can raise a concern confidentially if it is believed that someone is misusing RNLI information or systems/devices. Refer to Raising Organisational Concerns

2.12 Undertake education and awareness on security and using RNLI information and systems, including mandatory annual cyber security training, to support the understanding of recognising and reporting any threats, risks, vulnerability and incidents to the Information Security Team using infosec@rnli.org.uk.

3. Management responsibilities

Managers shall ensure that:

3.1 All staff/volunteers are aware of and understand their responsibilities outlined in this policy.

3.2 Any starters, movers or leavers in the team with access to systems or information are reported to People Admin in a timely manner to ensure access is changed appropriately or revoked by their last contracted day.

3.3 Team members only have access to information or systems that are required for their role and any excessive access is reported and removed.

3.4 Personal use of RNLI resources (e.g., internet browsing/streaming/downloads) are limited or managed appropriately.

3.5 All allocated devices, ID card and any physical information is collected / returned to the RNLI. Any non-compliance to return a device must be reported to IT Service Desk.

4. User IDs and Passwords

Users must:

4.1 Protect usernames, staff/volunteer numbers, entry access cards, dongles/USBs, portable hard drives and passwords appropriately.

4.2 Create secure passwords or a pass phrase that is at least 12 characters long and will be hard for anyone else to guess, but relevant to you, ensuring you can remember it. Passwords must not be stored in shared folders or written down.

4.3 Not use sequential letters, numbers or words that are easily associated with the RNLI, or other common words that would be easy to guess.

4.4 Immediately change their password if they feel their account has been compromised and report this to the IT Service Desk who will check account settings.

4.5 Not log onto RNLI systems using another user's credentials.

4.6 Lock their screen when temporarily leaving devices that are not in use whether you are at work, home or connecting elsewhere.

4.7 Log out of all computing devices, connected to the RNLI network, at least weekly or at the end of your working day.

4.8 Ensure that they enrol and use Multifactor Authentication (MFA) to help secure their account and RNLI systems and information.

If in doubt of how to set a strong password, please contact your Data Steward or email infosec@rnli.org.uk for assistance.

5. Use of RNLI devices, systems and networks

Users must:

5.1 Only use systems, applications, software and devices (including portable media devices, laptops and smart phones), which are approved, procured and configuration managed by RNLI IT, or approved suppliers, when undertaking RNLI business.

5.2 Ensure that the use of any computing (IT) equipment and data assets is done so in a responsible, professional, lawful and ethical manner.

5.3 Only use encrypted/secured portable media devices (e.g., USB/Memory sticks, SD cards, CD/DVD, Portable hard drives) where network connectivity is unavailable or very poor.

5.4 Always ensure that security and software updates are installed as this ensures the device has the latest security updates and will remain compatible with RNLI systems. To do this ensure the device is connected to the RNLI VPN weekly. Failure to do so may result in the device becoming restricted from access to RNLI resources.

5.5 Use Multifactor Authentication (MFA) to protect their account and in order to generate a text, call or authorise access, users are permitted to use a personal device where a RNLI device is not provided as part of the role.

5.6 Ensure they do not introduce malicious programmes or code into the RNLI network (e.g., viruses, spyware or malware).

5.7 Ensure that any 'protected' or 'classified' RNLI information is not shared externally without prior consent from the data owner. (Refer to Data Classification guidance.)

5.8 Ensure that RNLI devices are primarily used for business use, whilst occasional personal use is permitted.

5.9 Never tamper with the configuration of any RNLI device, either physically or logically, including installing unauthorised applications/software or disabling security measures such as anti-virous or anti-malware that is installed on the device.

5.10 Never remove any IT assets from their authorised and documented location, unless they have authorisation from the asset or process owner.

5.11 Never connect any unauthorised devices to the RNLI network without seeking approval from the IT Team first.

5.12 Never install any unauthorised software or application without prior approval from the Information Security Team and IT Team.

5.13 Never share privileged access or passwords to systems, network connections or system admins account, without prior approval from the Information Security Team.

5.14 Ensure that they connect their RNLI laptop to the RNLI VPN at least weekly, for a couple of hours, when in use to ensure that security and software updates are installed.

6. Internet and Email use

Users must:

6.1 Only use the internet or email communication within reason, ensuring it does not interfere with their daily duties or that of the RNLI resources.

6.2 Not use the internet to access prohibited content e.g., obscene material, gambling websites or illegal material, or to gain access to the dark web or any known malicious sites/applications.

6.3 Comply with Social Media guidelines, located on Compass, when accessing social media sites for RNLI work.

6.4 Only use RNLI email addresses for business use and never for personal use, including but not limited to access or registration to personal accounts, newsletter sign ups, etc.

6.5 Ensure that email communications that contain 'protected' or 'confidential' information is only shared between authorised parties and must be encrypted/secured. Where possible a secured shared link should be sent instead of any attachments or information recorded in the body of an email.

6.6 Not forward on emails that would be deemed as spam or phishing attempts to colleague's or any external contacts.

6.7 Not set up any automated forwarding rules on RNLI accounts to external email addresses, or manually forward emails to unauthorised external email addresses.

6.8 Consider that email correspondence may be read by a person other than the intended recipient (and may therefore not be private), and to exercise caution when using the internet and email.

6.9 Take care when opening emails and any attachments from unknown sources. If you have any doubts, contact the IT Service Desk or Information Security Team first.

6.10 Never distribute RNLI copyrighted material or in any way infringe any copyright, database rights, trademarks or other intellectual property.

6.11 Never inadvertently enter into contracts by email which bind the RNLI. Any contracts must be approved via the Procurement or Legal Teams.

6.12 Always connect to the VPN when using any public Wi-Fi or hotspot connection.

7. Physical and Travel Requirements

Users must:

7.1 Ensure that any RNLI equipment is always kept safe and secure and when not in use that it is hidden from view or at least placed in a locked and secured area.

7.2 Be aware of what could be observed from your screen when using your device at home or whilst commuting or travelling on business. If necessary, please contact IT for a privacy screen protector.

7.3 Ensure that their device(s) are locked when not in use to protect from unauthorised or inappropriate access.

7.4 Only ensure camera and/or screen shot facilities of the device are used for business purposes and will not identify people or protected/confidential RNLI information or that of any other business without authorisation to do so.

7.5 Ensure all devices are carried as hand luggage wherever permitted and where necessary protected from damage. Please check with the travel operator for any specific conditions prior to travelling.

7.6 Take responsibility to understand restrictions and limitations relating to the use of computer equipment in the country of destination. Refer to the HM Foreign Office website for more information.

7.7 Report any theft, loss or damage to equipment as soon as possible, providing full details to the IT Service Desk to enable us to block access to the RNLI network.
7.8 Take responsibility to keep secure any physical information classified as 'protect' or 'confidential,' to ensure it is not lost or stolen and securely shred/dispose of this when no longer required. Report it immediately to the IT Service Desk if lost or stolen.

8. Using your own (personal) device:

8.1 The RNLI allows limited use of personal devices to connect to RNLI resources for business use only.
8.2 Users must never screenshot, download, or store RNLI business information on their personal devices. Instead, you must only access business information in the RNLI environment and can connect as and when.
8.3 You can access RNLI emails and other applications using www.RNLI2.org.uk. This web address is not to be published outside of RNLI communication channels.
8.4 You can also install Microsoft Apps from the App Store or Apple Store for access to Outlook (email), Teams, One Drive and log in to your RNLI account.
8.5 You must never directly connect a personal device to a RNLI internet (ethernet) cable.
8.6 Personal devices can be connected to Lifeline via the allotted password for limited personal use. This password must not be shared generally and is only for those who are permitted to use it as connectivity to this can be monitored.
8.7 All use of RNLI resources that you access can be monitored, but this does not enable the RNLI access to your personal information or any other areas of your personal device.

9. Online Meetings

9.1 The RNLI's approved application for virtual online meetings is Microsoft Teams. This is the application to use when organising online meetings with internal or external participants.
9.2 Data protection regulations mean that recording online meetings is permitted only once consent has been obtained from all participants.
9.3 Recordings must only be retained in line with organisational retention policies.
9.4 For any other online meetings that are arranged outside of the RNLI and Microsoft Teams, please ensure you do not share protected or confidential information unless you are confident the channel is secure, by asking the meeting organiser or seeking advice internally via the IT Service Desk or Information Security Team.

Exceptions & Exclusions

Any exception or exclusions must be raised through the Information Security Waiver ticket located on IT Self Services. The process is available on the RNLI intranet. Security Waivers must be approved prior to any change in behaviour or practice/process taking place.

Compliance and Consequences

Adherence to this policy reduces the impact from.

- 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 our objective of saving lives at sea.

Information systems can be monitored to assure adherence to RNLI Policy. In the event of a data breach or other security incident, systems access may be revoked, services shut down and devices collected for investigation.

Failure to adhere to this policy may result in disciplinary action being taken which could lead to dismissal, including criminal prosecution.

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
Telecommunications Security Act 2021
Human Rights Act 1998

Related RNLI Policies, Procedures & Guidance (Located on Compass)	
Information Security Policy	**Mobile Device Process**
Disciplinary Policy	**Mobile Phone User Guide**
Social Media Policy	**Laptop/Tablet User Guide**
Mobile Device Policy	**Media User Guide**
Clear Desk Policy	**Data and Information Governance Policy**

Related RNLI Forms & Instructions (Located on Compass)
Information Security Waiver - Process and Form
Information Asset Register
Information Security Questionnaire (located on IT Self Services)