Policy Title & Version Number
Mobile Device Policy  V1.0

Policy Owner
Head of IT

Published Date
17 July 2018

Next Review Date
17 July 2019

Reason for Policy
The purpose of this policy is to promote and preserve the confidentiality, integrity and availability of information while in transit and at rest for mobile devices throughout the RNLI. The penalties for not keeping our data safe are extremely severe and failure to comply with this policy will lead to disciplinary action.

Objective of Policy
This policy outlines the obligations of RNLI personnel to sustain a secure network for all organisational mobile devices to connect to, and an individual’s responsibility to adhere to an acceptable level of behaviour, when issued with a mobile device that is required to fulfil necessary tasks of their particular role.

Applicability
This policy applies, irrespective of geographical location, to all employees, volunteers, contractors and temporary staff, within the organisation that are issued with a mobile device for RNLI business purposes. This policy must be adhered to at all times.

Types of devices include:
- Laptops
- Tablets
- Mobile phones (standard and smart phones)
- Portable Hard Drives
- USBs

Out of Scope:
CDs / DVDs / SD Cards. These are all data storage devices and must be kept safe and secure and disposed of correctly to ensure data, photos and videos are not compromised. Ensure that the User Guide is adhered to when using such media.

Connecting personally owned devices directly to the RNLI network for access to RNLI data or systems is not permitted without prior and specific authorisation of a Security Waiver Form.
## Policy

### 1. Policy Statement
A mobile device is any portable electronic equipment that could enable or provide access to our corporate network or data from any location. RNLI data such as; supporter data, financial data, HR data, intellectual property and sensitive commercial information e.g. board papers must be protected at all times. It is imperative that this information is appropriately safeguarded to reduce any risk or damage to reputation and brand of the RNLI, which is crucial to continued public support and donations.

Only approved devices may be connected to the RNLI network. The RNLI sees the supply of mobile devices as a valuable business aid however; these devices are costly and should only be approved where there is a business need for such a device to be allocated.

### 2. Policy Eligibility
Mobile devices and any associated equipment will be issued only with the prior approval of the appropriate line manager or departmental director, on the following basis:

- Where it is necessary to fulfil the requirements of a specific role; or
- Where the job involves significant travelling and contact with external organisations; or
- Where the safety of the individual is considered to be at risk, due to isolated working conditions

**Temporary allocation:**
A mobile device can also be available on a temporary basis for RNLI staff who occasionally have to travel on business, being placed on call or working away from the office.

### User Requirements
To comply with this Policy, you must ensure:

- Proper care is taken to prevent damage or loss/theft of the mobile device.
- Report any loss / theft of a device immediately to the IT Service Desk and your local police authority.
- Passwords and/or PIN numbers are not shared or disclosed to anyone.
- Lock away or tether the device when not in use.
- The device is maintained / updated with the latest version of the operating system.
- RNLI data is never stored on the device.
- No unauthorised software or content is loaded onto the device.
- Device systems and security settings are not changed unless expressly instructed and authorised to do so by a member of the IT department.
- The device is not used to store or transmit obscene, offensive, political, racial, or religious material, or for harassing, threatening or intimidating others.
- That the device is not shared with unauthorised persons.
- That a hand held device is never used while driving.
- That WiFi is used wherever available so as to reduce the costs of mobile data services.
- That when using a public WiFi connection you do not work on RNLI Confidential or Protected information without connecting up to the RNLI VPN access first.
- Any damage to a device is reported immediately to the IT Service Desk.
- Mobile device(s) are provided for RNLI business purposes and will be returned to your line manager / IT Service Desk when leaving the RNLI.
- Apps are only downloaded from recognised Apple or Windows stores. Any downloaded apps are only appropriate for work activity. You must also be aware of what access permissions you allow an app to have and ensure this will not enable sight of RNLI data. If you are not comfortable with the requested permissions of an app, please ensure you deny the request or search for an alternative app. Always ensure you are aware of risks
surrounding any apps installed or that you wish to download. Regularly review and clear out the apps no longer in use/applicable.

Technical Requirements (Configured by Supplier and/or RNLI IT)
- Devices must use the following operating systems: IOS or Windows.
- Devices must be configured with a secure password, which complies with the company standard.
- Devices must store all user saved passwords in encrypted form.
- Devices must have antivirus and firewall software installed.
- Devices must time out after a period of inactivity of 1 minute, forcing use of the password or PIN to gain access.
- Devices must be securely wiped of data before re-assignment, disposal or sending to a third party for repairs.

Governance Roles and Responsibilities
Responsibility for day to day compliance with this policy sits primarily with;
1. Individual users; that have been entrusted with an RNLI mobile device(s). Specific RNLI device user guides are also issued for each type of device allocated and must also be adhered to in all instances.
2. Line managers; must ensure they are aware of all devices in use by their team members at all times and that these are returned when no longer required or when a team member leaves the RNLI. For further information contact the IT Service Desk.

<table>
<thead>
<tr>
<th>Role:</th>
<th>Responsibilities:</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Day to day compliance with this policy and specific user guides.</td>
</tr>
<tr>
<td>Line Manager</td>
<td>Aware of team members with allocation of mobile devices.</td>
</tr>
<tr>
<td></td>
<td>Ensure collection of all devices from team members at the end of employment / contract. Return device(s) to IT for re-use / disposal.</td>
</tr>
<tr>
<td>IT Service Desk</td>
<td>Ensure that the RNLI IT Asset Register is updated accordingly.</td>
</tr>
<tr>
<td>IT Service Desk / IT Technical Teams</td>
<td>Ensure that appropriate line management approval has been granted in order to process device requirements.</td>
</tr>
<tr>
<td>IT Technical Teams</td>
<td>Offer technical guidance and assistance should technical requirements change.</td>
</tr>
<tr>
<td>Information Security Team</td>
<td>Ensure that all technical controls are in place before allocation.</td>
</tr>
<tr>
<td></td>
<td>Ensure mobile devices have the latest software updates.</td>
</tr>
<tr>
<td></td>
<td>Ensure all devices allocated are agreed with individuals / signed for.</td>
</tr>
<tr>
<td></td>
<td>Ensure that any non-compliance to this policy and user guidelines are escalated / investigated thoroughly.</td>
</tr>
<tr>
<td></td>
<td>Ensure that there is a valid and authorised Information Security Waiver recorded where any non-compliance to this policy has been approved.</td>
</tr>
</tbody>
</table>

This Policy shall be subject to audit by Internal / External Audit and external regulators as appropriate.

Exceptions & Exclusions
Any exception or exclusions to this policy must be raised through the Information Security Waiver Process, available through the RNLI intranet.

Consequences
Adherence to this policy reduces the impacts to;
- 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 and in the event of a security incident, systems may be shut down or devices obtained for further investigation.

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 References

- Computers Misuse Act
- All applicable UK, ROI, EU Legislations
- Foreign Office: It is your responsibility to check on relevant Legislation of a country you may be travelling to in order to adhere to local Legislations and not be found in breach of any Laws when using mobile devices or communicating information.

### Related RNLI Policies

- Information Security Policy
- Acceptable Use Policy
- Disciplinary Policy

### Supporting Documentation (Located on the RNLI Intranet)

- RNLI Mobile Device Declaration (Appendix A)
- Information Security Waiver - Process and Form
- Mobile Device Request Process
- Laptop and Tablet User Guide
- Mobile Phone User Guide
- Portable Media User Guide
Appendix A – User Declaration

RNLI Mobile Device Declaration
The mobile device and associated equipment to which this receipt relates will be provided to you in connection with your role, for use during your service with RNLI. You must confirm that you have read and understood the Mobile Device Policy and undertake at all times to keep the RNLI mobile device secure and use it in accordance with the Mobile Device Policy and relevant User Guide(s).

Declaration:
- I agree to follow all requirements set out in the Mobile Device Policy and all associated user guides for all mobile devices allocated to me as part of my RNLI role. This includes, but is not limited to the following:
  - Ensuring the device(s) is safe and secure at all times and not allowing others to use it/them.
  - Keeping the device(s) up to date with security requirements at all times. (Refer to User Guide)
  - Ensure the device(s) is only used for business, with minimal personal use.
  - To ensure that the device is used responsibly at all times in order not to put the RNLI network at risk to malware or viruses.
  - To ensure that any loss or damage to a device is reported immediately.
  - To ensure that all allocated devices are returned to the manager or IT Service Desk when leaving the RNLI.

I also agree that:
- Any unauthorised and/or excessive use that results in excess costs to the RNLI will entitle the RNLI to reclaim reasonable costs directly from salary.
- Any damage to a device that is deemed the fault of the user can also result in deductions from salary.

I am aware that any breaches to the policy etc. could result in the mobile device being recalled and alternative arrangements made.
I *agree/*disagree (*delete as appropriate) to comply with the Mobile Device Policy and relevant User Guide(s).

Signed (User):……………………………  Print Name: …………………………………

Date: ………………………………………

Note: Acceptance must be received prior to any device being issued or within 10 working days of a device being received or delays / impact to your working day may be experienced.

Response communications:
By Email: Please send your response to the IT Service Desk by either, using the voting buttons provided at the top of the email or, scan and email your signed declaration.
By Post/ In person: Please sign above and send/scan/deliver your acceptance to the above, to the IT Service Desk / Networks & Telecoms Team.

IT Use Only: (Details to be recorded in the IT Asset Register)

<table>
<thead>
<tr>
<th>Asset Type:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Tag / Serial No / IMEI:</td>
<td></td>
</tr>
<tr>
<td>Other items / ref:</td>
<td></td>
</tr>
</tbody>
</table>

RNLI Confidential