

Acceptable Use Policy		
-----------------------	--	--

Document Information

Owner:	Management Team
Author:	Nicola Dorrian-Clark
Approver:	Q4CL NI Trustees
Version:	1
Last Updated:	1 st October 2024

Version Control

Date	Version	Made By	Comments
1/10/24	1	Nicola Dorrian-Clark	New Document

Table of Contents

- 1 Objective 3
- 2 Scope..... 3
- 3 Responsibilities 3
- 4 Policy 4
 - 4.1 User IDs and Passwords..... 4
 - 4.2 Email Security 4
 - 4.2.1 Inappropriate Email Content and Use..... 4
 - 4.2.2 System and Network Activities 4
- 5 Reporting of Unacceptable Use 5
- 6 Review 5

Acceptable Use Policy

1 Objective

The objective of this policy is to ensure that everyone is aware of the acceptable use of information and other associated assets.

The purpose of having these controls in place is to minimise the risk of:

- Unintentional sharing of organisational or personal information.
- Data breaches of any of the systems or networks.
- Breaking the law.
- Reputational damage.

2 Scope

This document applies to all Q4CL NI trustees, volunteers, and any other individual working for or on our behalf who has access to Charity devices.

All equipment and information owned and controlled by us fall within the scope of this policy (including all information systems, hardware, software, channels of communication, social media, and email).

3 Responsibilities

Role	Responsibilities
Trustees	To be accountable for the implementation of this Policy
Management Team	To be responsible for the implementation of this Policy
Document Owner	To be responsible for the accuracy and integrity of the document To ensure the content is sufficient for the carrying out the actions the document specifies
Volunteers	To ensure they are aware and comply with this document and other related documentation.

4 Policy

4.1 User IDs and Passwords

You must:

- Protect usernames and passwords appropriately.
- Create secure passwords that are not stored in shared folders or written down.
- Do not log on to any charity systems using another user's credentials.

4.2 Email Security

Misused email can be a source of security issues for any organisation.

Users of the Charity's email system must not:

- Open email attachments from unknown sources (they may contain viruses, Trojans, spyware or other malware).

Any user who receives an email they consider to be potentially harmful should immediately report this to a trustee.

4.2.1 *Inappropriate Email Content and Use*

- Our email system must not be used to send or store inappropriate content or materials. Everyone must understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.
- Write or send emails that might be defamatory or incur liability for Q4CL NI.
- Send messages or material that could damage our image or reputation.
- To knowingly misrepresent Q4CL NI.
- Use email for any illegal or criminal activities.

4.2.2 *System and network activities*

Our systems have technical and organisational controls in place.

Users of the Charity's systems must not:

- Access Q4CL NI's assets or a user account for any purpose other than conducting Charity business.
- Introduce any form of computer virus or malware into the network or any other system.
- Distribute, disseminate, or store images, text or materials that might be considered indecent, pornographic, obscene, or illegal.

	Acceptable Use Policy	
--	------------------------------	--

5 Reporting of Unacceptable Use

Anyone who suspects unacceptable use should report this to a Trustee. All breaches will be investigated and reported to the appropriate authority.

6 Review

- This policy will be reviewed annually and updated as necessary.