# ICN IT Policy

| | |
|---|---|
| **Date of Last Review:** | **24.06.2024** |
| **Review Completed by:** | **Stephen Foster (COO)** |
| **Date Signed off by Trustees:** | **07.02.2025** |
| **Signed off by:** | **Alison Orman (Chair of Trustees)** |
| **Next review due on:** | **07.02.2026** |

## Contents

# Email Policy

## Introduction

This policy explains what is classified as the acceptable and unacceptable use of the ICN email systems and applies equally to all individuals granted access privileges to this resource.

### 1. Data Protection Act 2018 and The Human Rights Act 1998

ICN is committed to acting in compliance with both the Human Rights Act 1998 and the Data Protection Act 2018.

### 2. Use of ICN Email Application

The following procedures apply to all electronic media and services which are;

- Accessed from ICN premises, using ICN computer equipment, and/or used in a manner which identifies the individual with ICN.
- Accessed remotely e.g. from home, or whilst travelling on ICN business.

Third parties should not have access to the ICN email system.

**Policy**

- ICN email is provided primarily for ICN business activities.
- ICN email is not to be used for staff's personal use unless agreement has been given in writing beforehand by their Line Manager.
- If agreed by the staff member's Line Manager for them to use ICN email for personal use employees should make it clear that the email is a personal communication and not on behalf of ICN by stating at the top of the email ´non-ICN correspondence´.

### 3. Appropriate use of Email

Appropriate use of the ICN email system includes generating and sending emails regarding.

- ICN mission and program related activities.
- ICN business related and endorsed activities.
- Subject to Line Management agreement as outlined in this email policy statement, brief occasional personal messages.

### 4. Unacceptable Use of Email

**ICN email facility may not be used to:**

- Send email intended to intimidate or harass.
- Conduct personal business.
- Conduct political lobbying or campaigning unless aligned with the organisation's aims and values or on behalf of a service user (i.e. making contact with their local MP). Confirmation should be sought from the system user's Line Manager before doing so.
- Violate copyright laws by inappropriately distributing protected works.
- System users may not pose as anyone other than themselves when sending email, except when authorised in writing by their Line Manager to send messages for another user when serving in an administrative role.
- Email system users may not use unauthorised email software.

- Send or Forward chain letters junk or SPAM emails, unless doing so by a Manager to highlight a spam to delete if received
- Send or forward email that is likely to contain computer viruses.

Employees who inappropriately use ICN email systems may be subject to disciplinary action.

**5. Enforcement**

- All user activity on ICN IT assets can be subject to logging and review.
- Typically, if an inappropriate email is brought to our attention, the "sender" will be directed to retract the message by a member of the Management Team - Inappropriate or unauthorised email will be retracted by managers if the "sender" is not available.
- Extreme or repeated violation of this policy may result in the disciplinary policy being followed which could result in employment termination.
- Additionally, individuals are subject to loss of ICN IT access privileges, civil, and criminal prosecution.

**6. Legal Liability**

Employees should be aware of the legal responsibility for e-mail misuse as it rests with **both** ICN and the employee responsible. For instance, where an email contains a defamatory comment, or a comment which could be considered to amount to harassment then this could attract liability to both the author of the email and to ICN.

Similarly, employees and particularly Managers, should be aware that ICN can be held to be vicariously liable for representations made of contractual arrangements entered into by its employees, where it is reasonable for a third party to assume that the employee is acting with ICN's authority. Managers should take great care in relation to both external and internal e-mails which could be contractually binding.

# Internet Policy

**Overview**

This policy document delineates acceptable use of the Internet by ICN employees, volunteers, and contractors while using equipment, facilities, Internet addresses, or domain names owned, leased, or registered to ICN.

**1. Coverage**

Anyone who uses ICN equipment and facilities, and uses Internet Protocol addresses and domain names registered to ICN. This includes, but is not limited to:

- Full, part-time or zero hour employees.
- Volunteers authorised to use ICN resources to access the Internet.
- Departmental contractors authorised to use ICN equipment or facilities.

**2. Roles and Responsibilities**

**Managers are responsible for:**

- Managers of employees, volunteers, and contractors have the final authority in determining whether an employee requires Internet access to fulfill job requirements.

- Acquiring Internet access for employees and volunteers, as needed.
- Educating employees and volunteers on restrictions pertaining to personal use of ICN networks, systems, and other electronic resources.
- Determination of appropriateness of employees and volunteers use of the Internet. This includes judgment of the acceptability of Internet sites visited and the determination of personal time versus official work hours.

**System Users**

- Refrain from any practice that might expose, compromise, or otherwise jeopardise organisational networks, computer systems, data files, and other electronic resources.
- Understand legal requirements and limitations regarding access, protection, and use of data covered by the internal IT Policy.

**3. Policy**

**Internet Access**

Employees who do not require access to the Internet as part of their official duties, may not access the Internet using ICN facilities under any circumstances.

**4. Permitted Use**

**Acceptable Personal Use of Internet**

Occasional and minimal use of the internet for personal purposes in an employee's own time is understandable and acceptable where such use does not contravene this policy. However, in allowing this, ICN requires employees to act responsibly. Employees must never allow use of this facility to interfere with their job performance or work responsibilities. Employees who abuse this privilege may be subject to disciplinary action.

**Use of Internet and company networks for non-business purposes**

Since employees that use ICN Information Resources may be perceived by others to represent ICN, employees may not use the Internet for any purpose that could reflect negatively on ICN or its employees. Personal opinions expressed over the course of online communications activities should include a disclaimer stating that they do not reflect official positions of ICN. Communications published via ICN Social Media accounts should not express personal opinion.

Employees may not initiate non-work-related Internet sessions using ICN information resources from remote locations. For example, employees shall not log into organisational resources from home or other remote locations to engage in non-job-related activities.

Personal use of ICN Information Resources to access the Internet is restricted to approved users; it does not extend to family members or other acquaintances.

**5. Reasonable Security and Privacy Precautions**

- All ICN PC's and laptops must have ICN Management approved anti-virus software downloaded.
- Any company data posted on internal Web sites must not be available to access by a broader online audience than is appropriate for the materials themselves.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to ICN.
- All software used to access the Internet must be part of the ICN standard software suite or approved by ICN Management.

**6. Prohibited Use**

Employees may not use ICN Information Resources, either after working hours or on personal time, to:

- Access, retrieve, or print text and graphics information that violate the Acceptable Use Policy.

- Engage in unlawful activities or other activities that could in any way discredit ICN.
- Engage in personal commercial activities, including offering services or merchandise for sale, non-business-related online purchasing, and personal commercial advertising. Where online commercial transactions are permitted as part of legitimate job functions, transactions are subject to ICN procurement rules.
- Engage in any activity that would compromise the security of ICN systems, resources or networks.
- Endorse any product or services, participate in any lobbying activity, or engage in any active party political activity outside the scope of ICN's aims and objectives.
- Access or download video and voice from the Internet, except as part of an approved job function.
- Store personal files obtained via the Internet on ICN drives, servers, or other devices.

**7. Illegal Use**
An employee who is found using the Internet for illegal purposes will be subject to ICN's Disciplinary Procedure and, in addition, may be reported to the police.

- Data Protection Act 2018
- Telecommunications Act 1984
- Copyright, Designs and Patents Act, 1988 and subsequent regulations
- Computer Misuse Act, 1990
- Criminal Justice and Public Order Act 1994
- Race Relations (Amendment) Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000

**8. Enforcement**
Individuals using ICN equipment to access the Internet are subject to monitoring by management. User activities may be logged and reviewed. Use of ICN systems constitutes consent to monitoring.

All files and documents—including personal files and documents—stored on or transmitted by ICN Information Resources are subject to managerial review and may be accessed in accordance with this policy.

Violation of this policy may result in disciplinary action, including termination of employment for employees and contractors; additionally individuals are subject to loss of ICN Information Resources access privileges, and could be subject to civil and criminal prosecution.

# Social Computing Policy

***No manager, employee, volunteer, or contractor of ICN may use ICN IT resources for Social Computing purposes without specific written permission from their line manager or it being part of their job description. Once permission is given the line manager should be kept informed of the nature and extent of this kind of use during supervision meetings. If such permission is given the following policy pertains:***

**Overview**
Online social networking opportunities—including professional blogs and "microblogs," communities and forums, wikis, peer-to-peer file-sharing networks, and other channels of online discussion and interactive publishing—are increasingly common. These collaborative and interactive resources can profoundly impact the way that ICN employees work, interact, and support each other and the organisation.

The collaborative nature of social networking can represent a valid and valuable professional resource, providing ICN expert advice, technical knowledge, and innovative deliberation unavailable through internal organisational channels. However, interaction with a broad professional community outside of the ICN staff and network can also introduce risks. Employees who participate in social networking channels must interact responsibly and avoid actions that undermine productivity, expose proprietary information, or violate the privacy of ICN clients, Partners, and Employees.

**Coverage**
ICN respects the rights of employee´s right to personal privacy outside of the workplace; however, any employee publication, interaction, or online representation that references ICN in part or at any time is considered to be covered in its entirety by this policy.

**1. Policy**

**General Guidelines**
Good practices for social networking are consistent with general rules for professional communications and interactions. Employees are individually responsible for everything they publish to their personal online channels and should exercise good judgment in determining whether the information they release is professional, appropriate, and representative of ICN. In general, interactions with online communities or interactive publishing media must:

- Identify the employee by name and organisational role in any communications or publications about ICN or its initiatives.
- Be accompanied by a disclaimer that any views expressed are the employee's own and are not endorsed by or necessarily representative of ICN.
- Provide value in all interactions. This means that all social media content referencing the organisation should have a purpose and a benefit for International Care Network, and accurately reflect our agreed position.
- Adhere to principles of conduct and professionalism that govern other in-person and workplace communications. Do not publish abusive, harassing, defamatory, obscene, offensive, provocative, promotional, irrelevant, deceptive, or hateful content.
- Comply with conduct guidelines and applicable laws and contractual terms, including:
  - ICN code of conduct.
  - National copyright and fair use laws.
  - National and state privacy laws covering the disclosure of personal, proprietary, and health information.
  - Non-compete and non-disclosure agreements or contracts covering the employee and ICN.
  - National financial disclosure laws.
  - National or trademark, trade secret, and patent laws.

**2. Definitions**

**Social Networking Sites**
Minimal and occasional use of the internet for personal purposes to access Social Networking sites in their own time is acceptable, where such use does not contravene this policy. In allowing this, ICN requires employees to act responsibly and employees must not allow the use of this facility to interfere with their job performance or work responsibilities. Employees who contravene this principle may be subject to disciplinary action.

Social Networking sites that are updated on the behalf of ICN, will be subject to periodic review, to ensure published information does not bring ICN into disrepute and is in compliance with ICN's core values. The Communications team is responsible for setting up and managing International Care Network's social media

channels. Only those authorised to do so by the Communications Manager will have access to these password protected accounts.

Further guidance is available from the ICN Office and Communications Manager.

**3. Information Disclosure**

The following types of information may not be disclosed without explicit consent by the Office and Communications Manager:

- Conversations between employees.
- Announcements, documents, discussions, or other information shared in internal meetings.
- The names of clients, partners, suppliers, or other employees. It can be acceptable to use a pseudonym or generic description of an entity to illustrate a point or use case, as long as this reference does not by design or inference reveal the true identity of the referent.
- Internal emails, notes, memos, and other interpersonal communications.
- Internal documents not specifically marked for external distribution.
- Pre-publication drafts of documents ultimately intended for public distribution.
- Planning documents, production documents, software code,
- Organisational charts.
- Organisational contracts, policies, and other legal documents.

The following types of information may be freely disclosed without further authorisation:

- Information published by the press or other media outlets about ICN.
- Your own name and role (unless specifically prohibited by your manager or another organisational contract, policy, or guideline).
- Publicly available financial and business information pertaining to ICN.
- Best-practice knowledge, advice, and general professional insight that does not expose internal operational procedures or imply or disclose any proprietary or otherwise protected information.

**4. Conduct**

- Social Networking interactions must adhere to the ICN Code of Conduct, and should reflect common-sense principles of constructive professional communications. Employees should:
  - Truthfully represent themselves and their work, but protect their own privacy. Employees should not divulge details that would not normally be shared with colleagues or strangers.
  - Be considerate of others and conscious of the potentially global perspective that is often represented in social networking.
  - Keep internal communications internal, even when communicating with colleagues or other ICN employees.
  - Keep interactions professionally relevant. Avoid discussions of partisan politics, extra-professional groups or causes, personal activities, and lifestyle topics that might lead to unproductive debates or detract from other community members' ability to share professional knowledge. In particular, do not use the ICN name to endorse or promote any of the previously mentioned issues.
  - Speak as individuals and include a disclaimer, if possible, with any published information that clarifies the information, opinions, advice, etc. are their own and not posted on behalf of ICN.
  - Cite original sources when referencing or leveraging someone else's work. If possible, a link to an online reference for the source work should be included.
  - Respect the difference between professional enthusiasm and overt marketing or promotion. Employees should never promote ICN product, services, or events in forums where such promotion is culturally discouraged.
  - Avoid predictions and forward-looking statements about ICN financial performance, strategic decisions, leadership and business activities.
  - Keep communications positive and productive.

### 5. Enforcement

Violation of this policy may result in disciplinary action which may include performance sanctions; or in the case of a serious breach of these policies termination of employment; with the possibility of civil and criminal prosecution.

# Password Management Policy

### Overview

Account passwords are a mainstay of information security controls. This policy establishes management controls for granting, changing, and terminating access to automated information systems, controls that are essential to the security of ICN information systems.

### Coverage

All employees who use ICN Information Resources must have unique user account information, including passwords for access to various information systems. These procedures apply to accounts on all organisational systems: both in operation and in development.

### Roles and Responsibilities

The Manager overseeing IT Support (ITM) or if not specified the Office and Communication Manager (OCM):

- Provides management oversight of the process for administering passwords for ICN systems.
- Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords.
- Communicates to the users the system access and password requirements outlined in this policy.
- Liaises with the CEO when access is to be removed.
- Immediately informs the CEO if it is suspected that password has been compromised.
- Grants access and reviews access every year to determine continued need for access; and, if the need continues, re-approves through submission of System Access Request Form(s).
- Approves access of supervisor passwords and passwords for similar privileged accounts used on ICN's network.
- Issues passwords for privileged accounts to the primary system administrator and no more than one designated alternate system administrator; these passwords shall be subject to change when necessary due to employment termination, actual or suspected password compromise.
- Keeps the password protected Passwords spreadsheet up to date.

### Users

- Understand their responsibilities for safeguarding passwords.
- Use ICN data in accordance with job function and company policy.
- Understand the consequences of their failure to adhere to statutes and policy governing information resources
- Immediately notify ITM/OCM if it is suspected that their password has been compromised.

### 1. Policy Statement

All employees and personnel who have access to ICN computer systems must adhere to the password policy as approved by ICN and defined below, in order to protect and preserve ICN’s confidential data and intellectual property rights.

## 2. Password Requirements

The password security policy and security measures employed by the ICN are subject to regular review and updating by the ICN Management Team.

- Must include at least 3 random words, 1 number and 1 special character and be agreed by the Line Manager.
- Reset of locked out accounts to be requested and authorised by ITM/OCM.
- Passwords may not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.
- Passwords may not be visible on a screen, hardcopy printouts, or any other output device.
- Multi-factor authentication to be enabled for all staff who have access to ICN confidential information on the system.

## 3. Password Protection

- Any remote device accessing ICN's IT system must be password protected at all times. The remote devices' password protection is insufficient in itself. The ICN password protection must be activated at all times when the remote device is not being used for ICN work related activities – in other words the ICN account access should not be left open unless it is actually being used.
- Never write passwords down. Passwords are only to be kept on the password protected Passwords spreadsheet which is only accessible by the CEO and ICN Management.
- Never send a password through email, unless the email is encrypted and the document or file the password relates to is not included in the same email
- Never include a password in a non-encrypted stored document. (Post it Note, Desktop Diary, etc).
- Never tell anyone your password, especially over the telephone.
- Never reveal or hint at your password, especially on a form on the internet.
- Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- Report immediately any suspicion of your password being broken or being used to the ITM/OCM.
- If anyone asks for your password, refer them to your/their immediate Line Manager, or report the incident to the ITM/OCM.

## 5. Enforcement

Unauthorised personnel are not allowed to see or obtain sensitive data, which is critical to the security of ICN and its clients - employees that do not adhere to this policy may be subject to disciplinary action up to and including, prosecution for misdemeanour or felony, resulting in fines, imprisonment, civil liability, and/or dismissal.

## 6. Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

# Virus Policy

## 1. Preventative Measures

All ICN PC's and laptops will have ICN Management approved anti-virus software installed which will carry out full system scans regularly and automatically.

All software installed onto ICN hardware should be approved by the Manager overseeing IT Support (ITM/OCM) first.

Back up copies of core and corporate software applications will be stored in a safe back up hard drive connected to the CEO PC.

Central systems and software are backed up routinely to allow restoration of a system in the event of failure or infection by a virus. Information that is held remotely from the core systems is the responsibility of CEO.

Users will not be permitted to use their own copies of software on network connected systems unless explicit written permission is obtained from the ITM/OCM.

Viruses can be transferred by downloading documents from the Internet or from e-mail attachments.

### 2. Action in Event of Infection

Any system showing symptoms of possible infection must be reported to the ITM or a Line Manager immediately.

Any member of ICN implicated in the deliberate introduction of a virus, or the accidental introduction of a virus through failure to adhere to the preventative measures detailed above may be subject to ICN disciplinary procedures.

### 3. Guidance

The following guidance will help reduce the risk of infection:

- Ensure the ICN Management approved anti-virus software is installed on the ICN PC/laptop being used. Never boot a PC from a CD/DVD disk unless you are certain that it is virus free.
- Use write protect features on writeable CDs or DVDs whenever possible.
- Only use licensed copies of software obtained from a reputable source.
- Do not install any new software on the PC unless it has been virus checked first.
- Use password protection whenever it is available (PCs or network connections) to prevent unauthorised access to files.

In the event that you feel that your system has been compromised by a virus please use the following procedure.

- Inform the ITM/OCM or Line Manager of the problem as soon as possible.
- The ITM/OCM will assist with all investigations into the possible infection.
- **Do Not** propagate unsubstantiated information about virus infections.

# Service Users E-Safety Policy

### 1. Overview

The safety and security of our service users when using technology is paramount. It is essential that as part of ICN's support of service users, that appropriate training is given and the following policy is used. It is as important to make sure that devices provided by ICN for service users to use temporarily are set up properly and are used by the service users safely and securely. This policy is mainly relevant for departments that provide complete ongoing support to service users and where ICN devices are provided for them, such as Homework Club and to UASC young people under ICN support.

### 2. Roles and Responsibilities

CEO and Trustees: To annually review this policy.

Department Managers: It is the Department Managers responsibility to ensure that there are clear procedures for staff to follow with respect to training service users on how to use technology including internet, emails and online passwords. It is also their responsibility to ensure the ICN devices provided for service users are set up correctly with anti-virus software where possible and with the appropriate controls in place and to regularly check ICN devices to ensure they are being used responsibility and securely by service users.

Employees: It is the employees' responsibility to support their service users and train them on how to use technology safely and securely, according to their needs. Employees can use the department procedures to do this. It is also their responsibility to let the Department Manager know immediately if they notice any potential concerns or security risks with how the ICN devices are being used by service users.

### 3. Guidance

Support staff need to make sure that their service users:
- Password protect their devices and use multi-factor authentication where possible.
- Learn how to securely save passwords to accounts such as online banking and Universal Credit.
- How to identify, report (when possible) and delete scams including scam and virus emails.
- Know not to share their passwords with anyone.
- Know not to share their personal information with anyone apart from trusted services such as GP etc.
- Set parental controls.

For ICN devices Managers and staff need to ensure that:
- During particular sessions such as Homework Club, service users only use devices when necessary and are not left alone with the device and are monitored at all times.
- For ICN devices being kept at the UASC New Arrivals House, they should never be taken outside of the house by the service user and are only to be used for the purpose of learning, for example college ESOL study.
- If a device is given temporarily by ICN to a service user that a written agreement is signed stating that the service user will only use the device for learning purposes and will be responsible to replace device if lost or broken, unless agreed by the Department Manager.

# Additional Rules and Regulations

### 1. Software

Employees will not use the Internet to download entertainment software or games, to play against others across the Internet or participate in online gambling. Employees must not download software which may be used to access ICN's Office 365 system in order to determine employee passwords or to enable hacking into ICN's systems.

### 2. Defamation

Employees must not write, send, publish, copy, distribute or forward derogatory or defamatory remarks about any person or organisation either on the Internet or by e-mail. If an employee discovers potentially

defamatory material, then they should report it to their Line Manager immediately. Staff must not send or forward discriminatory messages, even if it is intended as a joke, as this could be regarded as harassment.

### 3. Offensive Material

It is unacceptable to access, archive, store, distribute, edit or record sexually explicit or other offensive material. An employee who inadvertently finds that they have accessed a site containing offensive or sexually explicit material must exit the site immediately and inform their Line Manager. If an employee is found to be accessing such sites regularly (more than once) and deliberately then they will risk disciplinary action and implementation of the ICN's disciplinary procedure.

An employee who receives unsolicited, offensive or sexually explicit emails should inform their Line Manager. It will be for the Line Manager to decide whether further investigation or disciplinary action is appropriate.

Unsolicited material which is circulated internally or externally, which has its origin internally or externally, may be classified as SPAM. Any employee who is found to be the originator of a SPAM attack from within the ICN, or using ICN equipment will be subject to disciplinary action by the ICN. This would have a severely detrimental effect on ICN's operations and on the credibility of the charity, its employees and its trustees.

### 4. Confidential Data

Accidental breaches of confidentiality can occur by entering a wrong address or forwarding a message to inappropriate recipients on ICN's distribution list. It is advisable when sending confidential or sensitive material by email that you ensure that it is encrypted and clearly states to the recipient that it is private and confidential.

### 5. Email Disclaimer

The following disclaimer shall be added at the end of each outgoing e-mail:

The contents of this email and any attachments are private and confidential. If you have received this in error please delete it and notify the sender. International Care Network is a Charitable Limited Company registered in England. Charity Registration Number: 1099400, Company Registration Number 04694225. Registered address: 200 Holdenhurst Rd, Bournemouth BH8 8AS. Telephone 01202 589395.