Connected Together
First for Community Engagement

# Information and Communication Technology - Use and Security Policy

| | |
|---|---|
| **Date approved by the Connected Together CIC Board** | December 2021 |
| **Version No:** | 6 |
| **Author/Responsible Person** | Michelle Wright |
| **Next revision due** | December 2024 |
| **Staff/volunteer training delivered** | Included in staff and volunteer induction and referred to as part of everyday practice |
| **Date sent to staff** | |
| | This policy covers Connected Together CIC and *all* its contracts and managed organisations, for example Healthwatch North Northamptonshire and West Northamptonshire (HWNW) and Healthwatch Rutland (HWR). |
| **Checked for rebranding** | Michelle Wright – 03 /05/2022 |
| **Signed off by CEO** | Kate Holt – 04/05/2022 |
| **Checked By** | Catherine Maryon (CTCIC Director) - date |

## 1. Purpose

The purpose of this policy is to ensure that all ICT (Information and Communications Technology) equipment used by Connected Together CIC, (from hereinafter referred to as CTCIC) and all contracts it holds is used effectively, safely, and legally to allow staff to carry out their duties and to further the aims of the organisation.

CTCIC recognises that the internet and the use of email and other electronic communications tools are crucial to conducting its business in an efficient way and for supporting its values, such as advancing knowledge, developing potential, developing business, and promoting quality of life. However, the use of IT resources raises a number of legal issues including confidentiality, data protection, copyright and harassment. There are risks attached to using these resources, and staff have an obligation to comply with current legislation and to reduce these risks by using resources sensibly and appropriately.

This policy outlines the standards for acceptable use of ICT resources. It covers many aspects of computer usage, including use of the internet, email, social networking, and data security. It should be read alongside the Data Protection Policy and Information Sharing Policy and Procedure.

If something is not specifically covered in this policy, staff should seek advice from their manager.

## 2. Scope

The policy applies to all staff, irrespective of their place of work, including home-based staff, temporary workers, and volunteers. Applicable sections (particularly 7, 8, 9, 10 and 12) also apply to Directors.

The organisation reserves the right to update or change this policy from time to time, as necessary, due to changing technologies and circumstances.

All changes to the policy will be clearly communicated to staff. Where appropriate, staff will also be consulted about changes to the policy in advance.

## 3. Communicating the policy

CTCIC is responsible for ensuring that all staff affected by this policy are aware of its contents and of their responsibility to use equipment appropriately. The policy will be communicated to staff through:

- induction briefing
- through periodic reminders to review and comply with the policy
- through provision of timely updates to staff whenever the policy is amended.

Volunteers and temporary staff will be given a copy of this policy on commencement at CTCIC.

## 4. Misuse of IT equipment

Failure to comply with the appropriate use of ICT resources may disrupt other legitimate IT uses and could lead to loss of business or cause the organisation's reputation to be damaged. In addition, use of ICT resources in breach of the organisation's policy may expose the organisation to legal liability.

Staff found using ICT resources in breach of this policy will be subject to disciplinary action under CTCIC's disciplinary procedure. This may result in suspension or loss of access to certain ICT resources, a formal warning, dismissal and/or legal action, as determined by the severity of the breach. The disciplinary policy states that 'Unauthorised use or misuse of Company property, equipment or resources' is an act of misconduct.

In situations where there is a reasonable belief that illegal activity has occurred, this activity may also be reported to the police.

## 5. Personal use of equipment

CTCIC permits reasonable, limited personal use of its equipment, which should only be undertaken during lunch breaks. Limited access to the internet or personal email during working hours, for example, can be seen to facilitate a work-life balance.

'Reasonable' use of equipment, including internet access, specifically excludes the use of systems by an individual to conduct his or her private business affairs.

'Reasonable' personal use of email is defined as the occasional sending and receiving of emails to and from private individuals not connected with the business purposes of CTCIC. This specifically disallows private emails containing confidential information, and defamatory or abusive emails.

'Reasonable' personal internet use is defined as occasional access to external websites not specifically related to CTCIC's business purposes. Staff may use the internet for occasional personal use during working hours, subject to the restrictions highlighted in the 'Internet use' section below.

'Reasonable' personal use of the telephone is defined as making occasional brief local/national calls during working hours which are non-work related. Staff may request to make long-distance or more costly personal calls, in which case his or her manager can arrange for these to be monitored for reimbursement.

'Reasonable' use of social media tools is defined as occasional viewing and updating of personal sites outside of the normal working hours. See the 'Social media' section for further details.

Staff should ensure that they take sufficient /appropriate breaks from the computer screen throughout the day, including lunch breaks. This to be agreed by their Line Manager. Uninterrupted use of the computer, for example, working on office-related documents all morning, then using social media or internet during the lunch break, can be detrimental to health in the long term.

## 6. Internet use

The internet is a largely unregulated space and poses a number of risks for individuals and organisations. CTCIC has a duty of care to protect its employees from being exposed to some of these threats. Web filtering software is used to eliminate as much offensive material as possible. However, staff should remain vigilant and not attempt to access illicit material if they come across it on the internet. This includes sites which contain obscene, pornographic, hateful, racist, or other objectionable content.

Staff should not download commercial software or any copyrighted materials belonging to third parties, (unless this download is covered or permitted under a commercial agreement).

The following activities are expressly forbidden:

- Visiting internet sites that contain obscene or other objectionable materials. The deliberate accessing or downloading of pornographic material is prohibited and is likely to constitute gross misconduct.
- Using the internet to send offensive, defamatory, or harassing material to other users.
- Using the computer to perpetrate any form of fraud, or software, film, or music piracy.
- Introducing any form of malicious software into the corporate network.

## 7. Email use

Email is perhaps the most prevalent communication method in the modern office. Its ease of use sometimes obscures the pitfalls which may result from its misuse. Email should be treated in the same way as any other form of written communication and staff should give it the same due care and attention with regard to content and presentation.

The following is a list of key Dos and Don’ts around email usage:

DO

- Ensure all emails sent to external recipients clearly identify the sender, including full name, organisation, and contact details.
- Inform the sender immediately and delete the message if you receive an email in error from an external recipient.
- Exercise care with cc messages. Before sending a reply to the original message, consider who is on the recipient list. Confidential information could potentially be disclosed to the wrong person by automatically including all of the original recipients in the reply.
- When communicating by email, no unauthorised person should indicate, either openly or obliquely, that they are entering into a binding agreement/contract, without the expressed permission of the CEO.
- If sending an email to a group of people, consider the use of the BCC method of copying them in on the email. In this way the recipients of the email will not be able to see the email addresses of the other persons to whom it has been addressed. In such cases, consider inserting the ‘enquiries’ (or similar e.g., ‘info@’ for HWR) mail address as the main recipient and BCC the remainder.
- If employees send personal data via email, it must be done using an attachment that is password protected. The password to the attachment should then be communicated by telephone or in a separate email.

DON’T

- Open anything which appears suspicious; it may contain a virus or other malicious code – if in doubt, delete the message. This applies in particular to messages received from unknown third parties.
- Make obscene or defamatory or otherwise offensive remarks about another person or company over email, even where distribution is restricted to the organisation, or forward such emails received to other addresses. Remarks of this nature may be construed as harassment.
- Forget that e-mail messages sent to external recipients via the internet are not secure. Sensitive or commercially valuable information should not be sent via unencrypted email. If complete confidentiality is required, confidential information must not be sent by email over the internet.

## 8. Social media

### CTCIC corporate social media use

Social media tools (Facebook, Twitter, blogs, wikis, etc.) play an increasingly important part in engaging with our members and the public online. They can bring the organisation much closer to its supporters and can provide instant feedback on issues which affect people.

However, by their very nature, these tools pose real security and reputational risks if they are not used in an appropriate way. Many of the caveats above regarding internet and email usage, such as avoiding defamatory or offensive remarks, apply equally to social media, which is essentially just another communications platform.

Only authorised staff should post to CTCIC/Healthwatch official social media accounts, such as Facebook and Twitter. Contributing staff should always be aware that they are representing the organisation and should adhere to the following basic rules:

- Postings should not bring CTCIC/Healthwatch into disrepute, for example by criticising colleagues or suppliers, making defamatory comments about individuals or other organisations or groups, or by posting images, or links to images, that contain inappropriate content.
- Confidentiality should be respected at all times; do not reveal confidential commercial or other information relating to CTCIC/Healthwatch or an individual working at the organisation or discuss CTCIC/Healthwatch internal workings or future plans which have not yet been communicated to the public.
- Do not breach copyright by using copyrighted images or written content without permission or by failing to give acknowledgement where permission has been given to reproduce something.
- Photographs are only uploaded with the consent of all those pictured, where it would be reasonably expected to do so.
- Any complaints that may be brought up on the site are responded to at the earliest opportunity, taken to a private communication channel and follow the organisation’s complaints procedure.
- Staff will not add any current volunteer, or service users they engage with during the course of their work on their personal account, as a Facebook friend; in order to maintain the appropriate service boundaries.

### Personal social media usage

It is also recognised that many staff use social media sites, including personal websites, for personal purposes. However, CTCIC must also ensure that confidentiality and its good reputation are protected.

Staff should follow these guidelines when using private social media:

- Do ensure that you conduct yourself in a manner not detrimental to CTCIC/Healthwatch.
- Be aware that social networking websites are a public forum, particularly if the employee is part of a ‘network’. Do not assume that postings on any social website will remain private.

- Restrict the amount of personal information supplied to these sites to minimise the risk of identity theft. Social networking sites allow people to post detailed personal information such as date and place of birth, and their pet's name, information which can form the basis of security questions and passwords on other sites.
- Do not use offensive or defamatory language on social media sites, or any language or behaviour that could be construed as harassment.
- Do not post sensitive, confidential, or corporate proprietary information on public forums, blogs or wikis.
- Do not do anything on these sites which could damage the working relationships between members of staff and members of CTCIC/Healthwatch.
- Do not download any software from social media sites, including plug-ins for games or other embedded features onto any office equipment.
- Do not publish defamatory or knowingly false material about CTCIC/Healthwatch, colleagues or customers on social networking sites, blogs, wikis, or any online publishing format.

## 9. Mobile device use

Mobile phones are provided by CTCIC on the basis of need to allow staff to carry out their duties effectively. Other staff may also choose to use their own personal mobiles for some work-related activities.

The staff member has a duty to ensure that company-supplied mobiles are properly safeguarded. Mobiles should not be left on open display, e.g. in unattended cars. A PIN number/biometric log in should be used to protect access to the device. If the device is lost, employees have the responsibility to report this to the Office Manager/CEO immediately within 24 hours that the loss is discovered. If the loss is due to the negligence of the user, CTCIC may consider the person responsible liable for the cost of its replacement.

Company-supplied mobiles may be used for private purposes as long as such use is kept to a minimum and does not interfere with business activities. Should excessive private use result in additional cost to CTCIC, e.g. the number of inclusive minutes is breached as a result, CTCIC reserves the right to reclaim the additional cost from the staff member responsible.

Do not use a mobile whilst driving. Answering and sending telephone calls, sending text messages, and accessing the internet, etc. while driving could amount to the offence of driving without care and attention or even dangerous driving. It is a criminal offence to use a hand-held mobile telephone or similar device while driving.

There may be times when urgent messages or calls require an instant response, in which case it is acceptable to take phones into a meeting and to step out in order to take a call or respond to a message. It is a common courtesy to refrain from sending or responding to text messages while attending a meeting. This courtesy should also be extended to other organisations when you are on their premises. Phones should be put onto silent if taking them into a meeting, and not be allowed to ring.

While mobile devices are provided to staff to allow them to carry out CTCIC's business efficiently, it should not be assumed that staff must be 'on-call' at all times of the day. Staff have the right to maintain a reasonable work-life balance, irrespective of the communications technology with which they are provided.

The downloading of 'Apps' onto smartphones is permitted with the proviso that such downloading does not breach any of the guidelines mentioned above. Any cost incurred will not be reimbursed by the company unless there is a clear business need. Where the cost of any app downloaded onto a CTCIC phone and does not qualify as a business use, it will be the responsibility of the staff member concerned.

### Mobile devices provided by staff

Staff may want to use their own personal devices to carry out CTCIC's work via our network. Third-party mobile devices, such as tablets or smartphones, will not be given access to the network unless they are fully consistent with our security protocols. CTCIC gives no undertaking to provide technical support for such devices even if they meet the security guidelines.

Some staff may wish to use their own personal mobile device to access work-related emails whilst out of the office. For example, staff attending conferences may wish to keep in touch with their office email while away from the office for a number of days. CTCIC will endeavour to accommodate requests to allow email access on personal mobile devices, but these must always be subject to security and support considerations.

## 10. Data Protection

The Data Protection Act 2018 (the UK's interpretation of the European GDPR) places strict legal requirements on the use, storage and transmission of data concerning living individuals. All staff have a duty to ensure that they comply with the provisions of the Act (See Data Protection Policy). CTCIC is the Data Controller.

Under our current guidelines all staff must observe their obligations under the Act which arise in connection with their employment, and are required to fully co-operate with CTCIC (as far as may reasonably be required) to assist it in complying with the Act as specified in the Information Governance Policy and as follows:

- All personal data stored electronically or manually is subject to the Act.
- Staff are not permitted to create and/or maintain private databases relating to individuals without the prior consent of the nominated Data Controller.
- Staff must comply with the company’s opting out/opting in provisions for any communications campaign (mailings, email campaigns, etc.) which they organise.
- It is the personal responsibility of any employee who needs to deal with any form of data to ensure that they have been advised of the relevant procedures and/or been given appropriate training.
- Staff should comply with CTCIC’s procedures for the collection of data via the telephone, email, etc. and ensure that third parties working on our behalf also observe these procedures.
- If in any doubt on any aspect of data protection, staff should seek guidance from their manager/data controller.

Employees who become aware of a breach, or a potential breach, of personal data, must follow the Data Breach Notification Policy

## 11. Copyright material

Downloading certain types of material from the Internet, or attaching copyrighted files or programs to emails, may amount to an infringement of copyright or other intellectual property right, or the breach of a license. CTCIC could be held liable, even where this behaviour was inadvertent. Therefore, staff must not make copies or download material or transmit such material unless they are absolutely sure that this is a permitted activity and is necessary for the purpose of their employment.

The use of unlicensed software on any of CTCIC’s computer systems is strictly forbidden. Software issued by CTCIC for staff use is licensed to the organisation and is protected by copyright law. If a member of CTCIC requires a specific item of software for the effective discharge of their role, they should consult with their manager/CEO before attempting to download any such software. If unsure the advice of a senior manager should be sought.

## 12. Harassment/abuse

ICT users must not send or request indecent, sexist, obscene, racist, or otherwise offensive material by email or harass, insult, threaten or intimidate colleagues or others by email or by any other electronic method. Any such activities may lead to disciplinary action being taken. Users must not send unsolicited mail (whether offensive or otherwise) or send or solicit bulk mail, chain letters, jokes, games, etc., which may cause aggravation or distress, lead to lost productivity, or introduce problems into the IT system.

## 13. Malware and viruses

'Malware' covers a variety of malicious programs which are designed to gain unauthorised access to systems, disrupt or degrade a legitimate service, compromise a user's privacy, or otherwise harms the computer user.

CTCIC maintains up-to-date anti-virus scanning software. Nonetheless, it is the responsibility of ICT users to exercise caution when opening emails received, especially where these are from unknown sources and/or contain attachments, and to notify our IT company or any accidental opening or downloading or suspicious material.

## 14. Security and passwords

To safeguard the network against external threats, CTCIC will implement regular password changes to maintain the integrity of the network access policy. Users must ensure that login and password details remain secure and are not advertised anywhere near the PC, nor given to other users (other than to authorised staff for support purposes). Do not use obvious passwords such as your own name, the name of children or pets, etc.

Users must log off from the network and switch off their computers before leaving the office at the end of the working day. During the day, users who are away from their desks should exercise caution when leaving their computers unattended, by closing down confidential documents and setting password-protected screensavers which run after a specified period of inactivity or locking their computers.

### Securing physical data

- Employees must not take 'hard copy' personal data out of the office, unless this cannot be avoided
- Employees must ensure 'hard copy' personal data is shredded before placing in the waste bin
- Employees must ensure that all 'hard copy' personal data is secured in locked filing cabinets
- Filing cabinets should never be left unlocked when the office is unattended. Keys should be locked away in the key safe whenever the office is unattended
- Access to filing cabinets that contain particularly sensitive information are restricted to those who need access only
- If personal data is no longer needed, employees must take responsibility for ensuring that it is deleted or disposed of in line with the record keeping and retention policy. Take advice from the officer manager if unsure.

## 15. Password Security

On initial setup, a new user will be supplied with a basic password to enable access to their machine. Once access has been established, the password word should be changed to one of their choice. DO NOT use obvious phrases etc. for passwords, such as children's' names, birthdates etc.

If you feel you have to make a note of the password, write down a cryptic clue that will jog your memory if you forget, rather than the password itself.

Do not allow internet browsers to remember your passwords for accounts that contain personal information, i.e. email and Civi CRM accounts (software package).

On no account give your password to any other person.

Should there be a need to access another user's computer, permission of a senior member of staff will be required. That member of staff will communicate with Indigo, and they will temporarily change the password for access to be achieved. When access is given, the person asking for permission, along with the senior member of staff, will be present whilst the information is obtained. Once done so, the original password will be re-instated, or a new temporary one will be given by Indigo. This new password will be given to the senior manager, who will then be responsible for informing the relevant staff member that their computer was accessed, and the reason.

Indigo will be informed that under no circumstances are they to allow access to another staff members computer, or divulge or change another's password, unless and until a request is made, via email, from a senior manager, using the senior managers computer/email account, so that a request can be verified.

## 16. Laptop and USB security

Staff may use CTCIC-supplied laptops to carry out work outside the office. Staff should take sensible precautions to safeguard equipment against loss, while in transit, at an external work location, and at home.

Confidential data, including information relating to staff/clients (see Data Protection Policy) should **not** be stored on laptop hard drives or unencrypted USB sticks. Files and data can be access from the shared network and CRM databases, which have sufficient security. If local copies are downloaded to the hard drive to work on, they should be deleted once they have been uploaded at the end of the session (before the laptop is switched off).

Where staff require confidential data/documents to be used on a laptop and they cannot access them from the shared network/CRM they should store the files on an authorised and encrypted USB stick and password protect the documents. This will ensure that any data lost on portable devices will not be accessible to unauthorised users.

Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying a manager or IT support immediately upon loss of a device.

**Own devices**

All the above also applies to the use of staff's own personal computer or laptop to work from home. Extra precautions should be taken if the device is shared with others.

## 17. Remote access to the network and email

All employees who require remote access to network resources from home will be given the relevant information from Indigo (IT support).

Staff can also access email from outside the office using Outlook Web Access/Office 365 via a browser.

Care should be exercised particularly if this service is accessed via a public computer. Ensure to log off when you have finished using remote access and close all windows to end the session. Passwords to the Outlook Web Access, Office 365, the file remote server and the CRM should **not** be stored on the laptop or in the internet browser memory.

Two factor authentication (2FA) should be used when accessing email accounts and can be set up for all users by Indigo. It is recommended 2FA is also used on other accounts, such as social media, to prevent unauthorised access.

## 18. Monitoring

Staff have a legitimate expectation of privacy. However, staff should be aware that many ICT systems automatically record user activity, e.g. logging of all access to websites, and passive monitoring.

CTCIC reserves the right to monitor the use of ICT resources and examine material stored on, transmitted through, or accessed from its facilities, and to carry out active monitoring if a user is suspected of serious violation of the acceptable use policy, in which case his or her right to privacy will be superseded by the organisation's requirement to safeguard its position.

Where appropriate, CTCIC will endeavour to inform an affected employee of the reasons for monitoring and how monitoring will take place. In such circumstances, the CEO/CTCIC Directors will guide and control the monitoring of other staff/the CEO and will agree which areas (e.g. email usage, web surfing, telephone calls, etc.) need to be monitored. The monitoring will be undertaken by Indigo, under the strict guidance and control of the CEO of CTCIC. Results of the monitoring will be reported back to the CEO for further action if necessary.
Examples of situations when active monitoring may be carried out:

- CTCIC has good reason to suspect that a staff member has been deliberately viewing or sending offensive or illegal material, such as racist or pornographic material. (This material may have been received or passed on inadvertently and therefore the staff member will be given an opportunity to explain if this is the case).
- CTCIC has good reason to suspect that an employee has been using the email system to send and/or receive an excessive number of personal communications or has been excessively accessing non-work related material on the internet, which would not be deemed 'reasonable' under this policy.
- CTCIC has good reason to suspect that the employee is sending or receiving emails that are detrimental to the reputation of the organisation.

In addition, if a staff member is absent for any reason, email messages may be checked to ensure that the business can run smoothly during their absence, e.g. details of contract negotiations may be contained in a user's mailbox. In such cases, a senior manager must give written authorisation to Indigo via email to grant access to the mailbox, and the affected staff member should be notified on their return that their mailbox has been accessed in order to retrieve business-related messages.

## 19. File storage

### Main drive partitions:

The main CTCIC/Healthwatch Drive is partitioned as shown below. All staff members must adhere to the protocols described.

### *Local drives: i.e. the 'C' drive.*

No information, files etc. should be saved to the local drive, as these local drives are not 'backed-up' and there is a risk of losing information in the case of a malfunction.

### *W: Drive*

These are the main drives for all CTCIC/Healthwatch documents, etc. and should be used to store completed work and any other relevant documents that need to be kept

Each member of staff can create their own personal folder in the 'W:' drive along with any sub folders within their main folder. In these folders they can store work which is ongoing and not yet ready for moving to the main folder.

Once a piece of work etc. has been completed it should be moved to the main folder.

The server is backed up automatically each night. The backup is stored offsite, so in the event of major fire, the IT part of the Business Recovery Plan can proceed once new equipment is in place.

Certain areas of the network are restricted to certain users, to limit access to authorised users only.

## 20. Disposal of hardware

All computer equipment which is obsolete must be wiped clean and disposed of securely, this is done by the IT company Indigo.

Related policies:

- Data Protection Policy-010
- Disciplinary Policy and Procedure-017