Christ Church Community Centre
Sedgemoor Road
Liverpool
L11 3BR
0151 226 2992
info@triplecliverpool.org

INFORMATION TECHNOLOGY USUAGE POLICY

Policy Adopted	September 2016
Last Reviewed	November 2022
Next Review Due	November 2025

Date Reviewed	Reviewed by	Approved by	Date Accepted by Trustees
01/11/2022	Operations Manager	Policy Review Committee	13th December 2022

INTRODUCTION

It is the responsibility of all users of Triple C (Liverpool), hereafter referred to as Triple C, Information Technology (IT) equipment and software to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1. PURPOSE

The purpose of this policy is to ensure that those with access to the organisation's IT equipment or software, (Microsoft Office 365, email, internet, computers, tablets, smart phones etc) understand the way IT should be used. It aims to ensure that all IT equipment and software is used effectively for its intended purpose without infringing legal requirements or creating unnecessary risk.

If an employee, trustee or volunteer chooses to use a personally owned device for charitable purposes, they must also adhere to the good practice outlined in this policy to ensure the safety, security, and protection of Triple C.

2. SCOPE

All employees, trustees and volunteers with access to IT Equipment or Software owned by Triple C are subject to this policy. Failure to comply may lead to disciplinary action, including dismissal. At the same time, your conduct and/or action(s) may be unlawful or illegal and you may be personally liable.

3. IT SECURITY

HARDWARE: LAPTOPS AND OTHER IT DEVICES

This covers all devices owned by Triple C or personally owned that are used to carry out work on behalf of Triple C.

Laptops and other portable IT devices are full of exclusive organisation information and must be handled with caution. As employees, trustees and volunteers often work from outside the office and from home, they must ensure that all devices are stored securely. If a device is lost or stolen it is essential to report the loss immediately to the Operations Manager), in their absence the chair or vice chair of trustees. Having a device lost or stolen is of course not a disciplinary matter, but failing to report the loss immediately is.

All devices must be password protected and the user is responsible for this and for the protection of their password.

All devices - computers, laptops, phones and other IT equipment given to an employee by Triple C for the purpose of work remain the property of Triple C and at the termination of employment should be returned to Triple C

Limited personal use of computers is permitted providing it:

- Is not illegal
- Does not adversely affect other users
- Does not interfere with work
- Or in any other way breach the conditions of this policy

SOFTWARE

This covers proprietary software or macros used for the purpose of carrying out work on your device for Triple C.

All hardware should include Avast anti-virus protection to minimise the risk of software or data corruption. It is recommended that windows security provided is also used It is also good practice to have other anti-malware protection that could prevent unauthorised access. Such software should be regularly updated and should not be disabled whilst your device is in use.

Any new software to be added to your device must be first approved by the relevant trustee and virus checked before it is installed on your device. Unauthorised software may compromise your ability to carry out work for the Charity.

Any software held on your device must not be modified in any way that would void the manufacturer's warranties.

DATA FILES

This covers files or documents, e.g. spreadsheets, PDFs, Word documents, and are typically used by the software on your device.

All files and folders must be saved in the Triple C OneDrive or SharePoint to ensure we can secure of all Triple C information in the event that a Laptop or mobile device in lost or stolen.

All sensitive data files, i.e. files containing personal information or information that should be protected from unauthorised access, must be protected by password.

Whilst working on your device we recommend that you turn autosave on and ensure that your work is saved on OneDrive or SharePoint. There is a possibility that data files could accidentally be deleted or your device becomes faulty. In some cases, there are existing mechanisms or processes in place that take automatic backups or data is shared and can be quickly recovered in the event of device faults or accidental file deletion. However, there may be no such mechanisms in place to quickly recover lost data and restoring data files from scratch would pose a significant burden.

4. USE OF INTERNET

Triple C provides Internet access to support its activities and access to this system is granted to employees, trustees and volunteers on this basis. Occasional personal use of the Internet is permitted in your own time but is limited to tasks that cannot be done outside normal working hours. Personal use of the Internet must not detrimentally affect the job responsibilities of other employees, disrupt the system and/or harm the reputation of Triple C.

5. INTRODUCTION TO GOOD PRACTICE PRINCIPLES WHEN USING EMAIL AND THE INTERNET

All employees are expected to adhere to our Good Practice guide. Some of the principles outlined in this introduction are developed in more detail later in the policy.

- Exercise due care when writing an email to avoid being rude or unnecessarily terse and ensure that your message meets the standards of professionalism Triple C expects of your position.
- Do not make any statements on your own behalf or on behalf of Triple C, which do or may defame libel or damage the reputation of any person.
- You should not engage in any activity that is illegal, distasteful or likely to have negative repercussions for Triple C
- You must not upload, download, use, retain, distribute or disseminate any images, text, data, videos, software or similar which:
    - Are or might be considered to be indecent, obscene, pornographic or illegal
    - Are or might be offensive or abusive in that its context is or could be considered to be a personal attack, rude or personally critical, sexist, racist, or generally distasteful
    - Encourage or promote activities, which make unproductive use of Triple C time
    - Involve activities outside of the scope of your responsibilities – for example, unauthorised selling/advertising of goods and services
    - Might be defamatory or incur liability on the part of Triple C or adversely impact on the image of the Charity.

- Would be a breach of copyright or license provision with respect to both programs and data you cannot or are not prepared to account for.

The following activities are expressly forbidden:

- The introduction of any form of computer virus
- Forgery or attempts to read other users' mail without their express permission

All email messages that have been deleted from the system can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending email can be identified. Emails, both in hard copy and electronic form, are admissible in a court of law.

6. USE OF EMAIL

Triple C encourages all employees, trustees and volunteers with the relevant access to use email and the internet at work where this can save time and expense. However, it requires that employees follow the rules laid out in this policy. It is a term of each employee's contract that they comply with these rules, and any serious breach could lead to dismissal. Any employee, trustee or volunteer who is unsure about whether something they propose might breach this email and internet policy should seek advice from the operations manager or relevant trustee.

Care should be taken when using email because email messages are perceived to be less formal than paper-based communication and there is a tendency to be lax about their content. Bear in mind that all expressions of fact, intention and opinion via email can be held against you and/or Triple C in the same way as verbal and written expressions.

The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

Equally, if an employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, they should not forward it to any other address.

All employees are encouraged to take care when accessing email Internet sites (e.g. Gmail, Hotmail, Yahoo mail etc.) take precautions to avoid the spread of viruses.

Employees should not attach any file that that may contain a virus or other malicious software to emails, as Triple C (Liverpool) could be liable to the recipient for loss suffered. It is the employee's responsibility to ensure that Avast virus software installed on their computer is regularly updated.

Employees should exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses or may be malicious in other ways eg. phishing emails or internet scams. It is good practice for employees to report such concerns to their email provider or as outlined in https://www.gov.uk/report-suspicious-emails-websites-phishing

7. CONFIDENTIALITY OF EMAILS

All personal information relating to volunteers, staff, trustees or service users of Triple C is confidential. You are expected to treat electronic information with the same care as you would paper-based information, which is confidential. Keep all such information secure, use it only for the purpose(s) intended and do not disclose the same to any unauthorised third party.

Always keep passwords safe. You should not disclose it to anyone else.

If a document is highly confidential or sensitive in nature, you should password protect it. Do not forward, send or in any way disseminate such information that may compromise Triple C (Liverpool).

Ensure that you maintain confidentiality by not forwarding or sharing any client or other personal information that would violate the Data Protection Act or industry guidelines.

Always return any message received that was intended for another recipient. Delete any copies of misdirected messages. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

Where appropriate, verify the recipients of the email are approved to receive the information contained in the email, to avoid a breach of confidence.

8. SOCIAL MEDIA

Triple C (Liverpool) operates a Social Media policy which details more specifically our expectations in the use of social media whilst at or for work purposes. All employees are to adhere to this policy.

9. USE OF DATA STICKS AND OTHER PORTABLE MEMORY DEVICES

The policy provides guidance to employees on the secure use of mobile technology for carrying confidential, sensitive and Person Identifiable Data (PID).

USB memory sticks, are popular because of their small physical size and large storage capacity. This makes them very convenient devices for carrying files from one place to another. However, these very features have introduced new information security risks:

- Potential breach of confidentiality – if the mobile device is lost or stolen.
- Physical loss – being so physically small the memory stick can be easily lost.
- Access to information and emails through mobiles and tablets
- Virus transmission – memory sticks can introduce viruses onto a computer network.

USB memory sticks may be used for non-confidential information but should not be used in any Triple C hardware which does not have up to date antivirus software.

There are several main ways of preventing the loss of information:

- Avoid physically carrying such information
- Encrypting confidential, sensitive & Person Identifiable Data
- Setting secure access passwords or key codes for Mobiles/Tablets

Data Avoidance Confidential, Sensitive and Person Identifiable Data must not be stored or carried on non-encrypted mobile data storage devices.

10. MONITORING

All Charity resources, including computers, email and voicemail, Internet are provided solely for charitable purposes. At any time and without prior notice, Triple C maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems.

Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to scrutiny by Triple C. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.

In order to ensure compliance with this policy, Triple C may employ monitoring software to check on the use and content of email and Internet to ensure that there are no serious breaches of the policy. Triple C specifically reserves the right for authorised personnel to access, retrieve, read and delete any communication that is created on, received through or sent via the internet, to assure compliance with all Charity policies. Such monitoring will be used for legitimate purposes only.