



Document Title:	CCT IT Policy		
Document Number:	CCT 05	Page Number:	Page 1
Issue Date:	08.07.2024	Issue Number:	Version 4
Author:	SW	Authorised:	Trustees

Chesterfield Canal Trust Ltd. IT Policy

1. Introduction

This policy sets out the expectations on employees, Trustees and volunteers of CCT including contractors and temporary staff, who use the organisation's IT facilities. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them. All users are responsible for IT activity which is initiated under their username.

2. Legislation

All users shall comply with the relevant legislation. This includes the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer misuse Act 1990
- Copyright Design and Patents Act 1998
- Defamation Act 1996
- Terrorism Act 2006
- Telecommunications (Lawful business Practice) (Interception of Communications) Regulations 2000
- Charities Act 2011

3. Passwords & Workstation Security

Access to CCT computer systems is secured by user passwords.

- Passwords must not, under any circumstances be given, or made available to others.
- If anyone using a CCT system suspects their password has been compromised, they must change it at once and report this.
- Passwords should not be stored adjacent to workstations etc.
- Passwords for systems must not be sent by email.
- Passwords should be a minimum of 8 characters and contain upper and lower case characters, numbers and symbols.
- If a password is to be shared, consider using a blind text or a phone call to the recipient. Do not send it by email.

4. Use of the Internet

Use of the Internet on the Trust's computer systems is an essential part of the smooth running of the Trust. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring the organisation into disrepute.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material.



Document Title:	CCT IT Policy		
Document Number:	CCT 05	Page Number:	Page 2
Issue Date:	08.07.2024	Issue Number:	Version 4
Author:	SW	Authorised:	Trustees

- Users must not knowingly introduce any form of computer virus into the CCT computer network.
- Users must not download software or any copyrighted materials belonging to third parties.
- Users must not use the internet for personal financial gain, nor for illegal or criminal activities, such as software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.

5. Good Practice

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for. Emails containing confidential information should be password protected. Caution must be used when opening any attachments or emails from unknown senders. Users must use their best endeavour to ensure that any file downloaded from the internet is done from a reliable source. Any concerns about external emails, including files containing attachments, must be discussed with CCT IT personnel.

6. Email address

Non CCT email addresses are personal data. They should therefore not be shared with other persons without their permission. When sending an email to multiple people, use the BCC function to prevent personal data being shared.

7. Network Drives and Storage Standards

Local C: drives should ideally not be used for storing critical data, as in the event of hard drive failure, the information will not be backed up and will potentially become irretrievable. Where data is stored on external devices such as an external hard drive or memory key, it should be kept securely with a separate log of what is stored on the device.

8. Loss or theft of hardware or data

All users issued with hardware must to be conscious of the security of the equipment and data stored on it at all times. These devices must not be left in a public place where they can be stolen or damaged and confidential organisation information viewed by unauthorised parties.

In the event that any device is lost or stolen, or in the event that passwords for cloud computing have been compromised, the user must contact the Chair of the Trust or the Trustee responsible for IT provision as soon as possible and explain what has happened so measures can be taken to protect the systems.

9. Remote Users

Users may sometimes need to use CCT equipment and access the CCT network whilst working remotely, whether from home or while travelling. The standards set out in this document apply equally when using equipment or resources other than that provided by CCT



Document Title:	CCT IT Policy		
Document Number:	CCT 05	Page Number:	Page 3
Issue Date:	08.07.2024	Issue Number:	Version 4
Author:	SW	Authorised:	Trustees

10. Account Closures

When an employee or Trustee is due to leave CCT, they will be requested to ensure that all work-related computer filing is completed and files remain accessible to their line manager. At a pre-determined time, their IT account and related email accounts/passwords will be terminated by CCT.

11. Use of Own Equipment

CCT understands that due to the nature of its operations volunteers will be using their own IT equipment. It is recommended that such equipment is kept up to date with security and anti-virus updates where possible. It should be noted however that where personal equipment is used to access CCT data that any credentials used to access that data should be treated as per the passwords policy above. Where data is downloaded it should be kept secure and removed once it is no longer needed. If a user suspects any data relating to CCT has been breached on their own equipment they should inform the Chair of the Trust and/or the Trustee responsible for IT provision.