# Acceptable Information Technology Use Policy

Croydon Drop In
Tel: 020 8680 0404
Company Limited by Guarantee Registration Number 3092355
Registered Charity Number 1049307
Registered Office, 132 Church Street, Croydon, CR0 1RF

# Acceptable Information Technology Use Policy

## 1. Introduction

It is the responsibility of all staff, volunteers and trustees at Croydon Drop in (CDI) to read and understand this policy. This policy may be updated from time to time in order to comply with legal and policy requirements. All CDI staff, volunteers and trustees must adhere to the provisions of this policy and all associated CDI policies.

CDI seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting and delivering its service to the highest possible standards. This also requires the appropriate and legal use of the technologies.

## 2. Purpose

This policy is intended to provide a framework for the acceptable use of all of CDI's information technology resources, this includes, CDI's Network, software and hardware, such as desktop computers, cameras, sound recording devices, laptops and all mobile computing devices (including Bring Your Own Device BYOD), telecommunications and email, website and social media platforms. It should be interpreted such that it has the widest application and so includes new and developing technologies and uses, which may not be explicitly referred to. CDI also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "Prevent". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

## 3. Definitions

CDI's Network refers to all computing, telecommunication, and networking facilities provided by CDI, with particular reference to all computing devices, either CDI owned or personal, connected to systems and services supplied.

For the purpose of this policy, 'mobile computing devices' refer to all forms of portable computing equipment that can store digital data. Examples include, but are not limited to, laptops, netbooks, tablets and mobile phones.

## 4. Acceptable IT use

CDI's Network may not be used directly or indirectly by staff, volunteers and/or trustees for the download, creation, manipulation, transmission or storage of:

- unlawful material or material which advocates or promotes any unlawful act
- material that brings the Charity into disrepute
- confidential material concerning the activities of the Charity
- offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise
- material that is abusive or threatening to others which is subsequently used to facilitate harassment, bullying and/or victimisation of others
- material which promotes discrimination on the basis of race, ethnicity, gender, religion or belief, disability, age, sexual orientation, marital status or political beliefs
- defamatory material or material that includes claims of a deceptive nature
- material with the intent to defraud or which is likely to deceive a third party

- the unauthorised provision of access to the Charity's services and facilities by third parties
- activities that violate the privacy of others or unfairly criticise or misrepresent others, this includes copying distribution to other individuals
- Material that infringes the copyright of another person, including intellectual property rights or privacy rights
- Unsolicited 'nuisance' emails, which is designed or likely to cause annoyance, inconvenience or anxiety. Including unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind.

CDI's Network must not be deliberately used by staff and/or trustees for activities having, or likely to have, any of the following characteristics:

- Intentionally wasting staff effort or other CDI resources
- Corrupting, altering or destroying another User's data without their consent
- Disrupting the work of other Users or the correct functioning of CDI's Network
- Denying access to the CDI Network and its services to other users
- Pursuance of commercial activities (even if in support of CDI's work), subject to a range of exceptions.
- Any breach of industry good practice that is likely to damage the reputation of CDI's network will also be regarded as unacceptable use
- Where CDI's Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the CDI's Network.

Staff, volunteers and/or trustees shall not:

- Introduce data-interception, password-detecting or similar software or devices to CDI's Network
- Seek to gain unauthorised access to restricted areas of CDI's Network
- Access or try to access data where the User knows or ought to know that they should not have access
- Carry out any hacking activities; or intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.
- Use personal email addresses at any time in work-related correspondence.

Exemptions from unacceptable use:

There are a number of legitimate activities that may be carried out using CDI's Network that could be considered unacceptable use, e.g. research for CYPF activities and/or campaigning. These may involve defamatory, discriminatory or threatening material, the use of images which may depict violence, the study of hate crime and/or terrorism related material. In such circumstances advice must be sought from senior management. Any potential research involving obscene or indecent material must always be discussed in advance with senior management. If a member of staff believes they may have encountered breaches of any of the above, they should make this known to the appropriate manager.

## 5. Email

CDI's main purpose in providing IT facilities for email is to support staff in the approved business activities of the Charity, communicating internally and externally with other agencies and children, young people and families.

CDI email accounts are securely maintained by CDI's IT provider, SME. When working remotely, CDI users can securely access their email accounts through the email provider. All members of staff will be allocated email accounts using the required and appropriate format at the beginning of their employment. Email names will not be changed for arbitrary or trivial reasons and the final decision on whether a reason is valid lies with senior management. All accounts have quota limits placed on them. Regular back-up procedures are in place. Accounts that are removed e.g. at the end of employment, will be archived in accordance with the data retention procedures.

All email communication through the CDI's Network email gateway is checked for malware and viruses. Checking strategies include, refusing messages containing executable attachments, scanning messages for known malware or a combination of both techniques. Messages containing malware will be reviewed CDI's IT provider. The sender of such messages will be informed of the viral content of their email. Spam can be defined as 'the mass electronic distribution of unsolicited email to individual email accounts'. Junk mail is usually a result of spamming. In reality, spam and junk mail are regarded as interlinked problems. CDI's IT provider has provisions in place to block junk mail.

## 6. Mobile Computing, Video and Sound Recording Devices

All equipment supplied to CDI staff and/or volunteers remain the property of the Charity. All equipment must be returned to CDI on request or on termination of employment.

All CDI electronic and IT equipment should be used for the intended business need. The security of any CDI data stored on all devices is vital and data protection laws must be followed at all times. Any unique data generated on such a device should be copied onto the appropriate CDI data store at the earliest opportunity to ensure information is backed up securely.

CDI's IT provider is responsible for maintaining the function, compliance with the appropriate license(s) and security of all mobile computing devices supplied to the Charity. Antivirus/antimalware software is regularly monitored and updated when required. If a User has any reason to suspect that their device has become infected with malware, they should immediately cease to use it, and with management permission contact CDI's IT provider to arrange for the mobile computing device to be cleaned/repaired.

Users should seek permission from management before passing on, discarding, or otherwise disposing of, any mobile computing device.

## 7. Information Security

All CDI staff, volunteers and trustees must ensure that passwords for highly privileged systems accounts, social media accounts and infrastructure components are changed from default values and have high strength. It is required that all CDI staff, volunteers and trustees have an understanding of good password practice.

Users are responsible for the physical security of their mobile computing devices and any CDI data stored on it. Information being accessed or processed using mobile computing devices should be treated in accordance with the GDPR and data protection policy.

Users of mobile computing devices should ensure that they have familiarised themselves with their device and ensure they have put in place the required security protection measures.

There are increased security and reputational risks associated with the processing of any data classified as 'restricted' or 'highly restricted' so users of all devices should give serious consideration before removing such data from within the safety of CDI's Network. For 'highly restricted' information, Users should consider encryption of the data.

All devices used in pursuance of CDI work must have remote wiping agents installed upon them to ensure sensitive data can be removed securely should the device be lost or stolen. Owners are responsible for ensuring that remote wiping agents are installed by CDI on their Bring Your Own Device (BYOD) if they intend to hold highly restrictive data on them. Owners are also responsible for backing-up any personal data stored on the device to allow for remote data wiping in the event of loss and/or theft.

Any loss of any device (including BYOD) or suspected breach of information security should be reported immediately to senior management. Suspected theft of a device (including BYOD) should also be reported. In the event of loss of devices, Users should anticipate that the Charity will take steps to mitigate the risk of any potential information security breach by the remote wiping of equipment. In such an event, any personal data the User has stored on the equipment will also be deleted.

Users should avoid internet café and other public Wi-Fi connections as these pose information security risks and should be avoided especially when accessing highly sensitive information.

Users of BYOD devices are responsible for ensuring that they maintain anti-virus software, operating systems and security updates, as appropriate to the equipment, if they use it to access, store or process CDI data.

CDI may monitor and log network usage as a means to protect information.

## 8. Roles and Responsibilities

The Board of Trustees and the Senior Leadership Team are responsible for approving and regularly reviewing this policy and all related policies. All CDI staff, volunteers and trustees have a duty to ensure they practice appropriate and proper use and must ensure they understand their responsibilities in regards to Information Technology. All staff and volunteers are required to undertake appropriate training when required.

## 9. Breaches and incident handling

In the event of a breach of this Acceptable Use Policy by staff, volunteers and trustees, CDI may in its sole discretion:

- Restrict or terminate a User's right to use the CDI's Network
- Withdraw or remove any material uploaded by that User in contravention of this policy
- Where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.
- In addition, CDI may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Policies and Procedures.

## 10. Additional information

This policy should be read in conjunction with the following:

- CDI Privacy Statement
- CDI Confidentiality Policy
- CDI Safeguarding Policy
- CDI Data Protection Policy (Appendix A CDI Data Retention table)
- CDI Data Incident Policy
- CDI Business Continuity Plan
- CDI Risk Register

| Policy Review Schedule | | | | | |
|---|---|---|---|---|---|
| Policy Reviewed by | Date Reviewed / Amended | Policy Approved by | Date Approved | Approved Signature | Review Date |
| Gordon Knott | 22.01.24 | Trustees | 18.3.24 | GK | January 2025 |