

Chapter One - Information Security Policy

Overview

Chapter One holds personal data about our employees, volunteers and teachers/pupils/parents participating in our programmes. We are trusted to keep this personal data safe and under a legal obligation to do so.

It is ultimately the responsibility of everyone who has access to our systems and information to keep all information safe and secure and therefore it is important you read and understand this Policy. Compliance with this Policy is also a contractual requirement of contractor and employee contracts and failure to comply could result in disciplinary or other actions.

What do I need to do?

- Be vigilant and aware of keeping information secure. Be alert for phishing scams.
- If you are asked to share any information with someone, please check that they are authorised to access such information and it is necessary for them to have it.
- When feasible, use strong passwords that meet the company standard (at least 8 characters, including one upper case letter and one number) and regularly update your password.
- Do not keep personal data from Chapter One on personal devices. If emergency use of a personal device is necessary, follow guidance in Section 7, and ensure you always sign out of Chapter One accounts after use.
- When sending important or sensitive information to anyone outside of Chapter One, make sure you protect it and send it securely e.g., encrypt documents with a password. Be very careful in your use of 'cc' and 'bcc' on emails to make sure data is not inadvertently shared more widely than it should be.
- If you become aware of any vulnerabilities or security breaches including suspecting that an unauthorised person has access to information or that information has been lost or stolen, please follow the Data Security Incident Response Policy.

Where can I find more information?

Please refer to more detailed information in the Information Security Policy. This Policy should be read in conjunction with other related policies:

- Chapter One UK Computer Use And Online Safety Policy
- Chapter One UK Access Controls Policy
- Chapter One UK Asset Management Policy
- Chapter One UK Data Security Incident Response Policy
- Chapter One UK Data Management Policy

In addition, if you have been issued with a Chapter One device (e.g., laptop/phone), you must ensure you comply with the device ownership, care, usage, and confidentiality rules in the Chapter One Staff Laptop/Phone Agreement.

Policy

1. Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of the company's information and assets. These rules are in place to protect customers, employees, and the company. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, financial and reputational risk, and legal and compliance issues. The company "Information Security Policy" consists of this policy and all company policies referenced and/or linked within this document.

2. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct company business or interact with internal networks and business systems, whether owned or loaned by the company, the employee, or a third party.

All employees, contractors, consultants, temporary, and other workers at the company and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources in accordance with company policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, and other workers at the company, including all personnel affiliated with third parties. This policy applies to all company-controlled company and customer data as well as all equipment, systems, networks, and software owned or leased by the company. All company-owned devices, networks, and systems are subject to monitoring and audit.

3. Roles and Responsibilities

It is the responsibility of all Chapter One employees to keep our information and systems safe and secure. Specific responsibilities are outlined in the table below:

Roles	Responsibilities
Chapter One UK CEO	• Data Protection Lead for the organisation • Ultimately responsible for the: ○ execution of information security and privacy risk management. ○ alignment of Information Security Policy with the company's strategic objectives and Risk Register ○ reviewing vendor service contracts ○ ensuring staff compliance qualifications.

	• The final authority for approving all policy exceptions and risk acceptances, based on a formal technical assessment.
Chapter One US Security Delegate (Chapter One US)	• Oversight over the implementation of information security controls for infrastructure and IT processes • Responsible for the design, development, implementation, operation, maintenance, and monitoring of IT security controls • Communicates information security risks to executive leadership • Reports information security risks annually to company leadership and gains approvals to bring risks to acceptable levels • Coordinates the development and maintenance of information security policies and standards • Oversight over Identity Management and Access Control processes, assists with secure configuration and monitoring • Responsible for the design and monitoring of development and commercial cloud hosting security controls • Responsible for oversight over policy development related to systems and software under their control • Responsible for implementing risk management in the development process aligned with company goals. • Oversight over information security in the software development process • Provides a mandatory, independent technical risk assessment for all policy exception requests;
IT Manager (System Owner)	• Manages access to specific platforms in line with the Access Control Policy • Approves access requests • Keeps records of all exceptions and necessary logs and reviews • Liaises with Security Delegate for technical advice as required • Supports staff and line managers as required
Line Managers	• Requests access for staff to specific platforms in line with the Access Control Policy • Liaises with IT manager as required to ensure staff receive accurate information about information security

Staff	• Adheres to company policies and standards of conduct. • Reports incidents and anomalies. • Helps identify and minimise risks.
-------	---

4. Security Incident Reporting and Business Continuity

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately in accordance with the Data Security Incident Response Policy.

Chapter One has in place appropriate systems and controls to ensure that business continuity is assured in the event of a technology failure or information security incident. Please see the Business Continuity Plan for more details.

5. Whistleblower Anonymous Reporting

Our Chapter One Whistleblowing Policy is intended to encourage and enable employees and others to raise serious concerns internally so that we can address and correct inappropriate conduct and actions. It is the responsibility of all employees to report concerns about violations of our code of ethics or suspected violations of laws or regulations that govern our operations.

6. Device Policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. See Computer Use and Online Safety Policy for more details.

System-level and user-level passwords must comply with the Chapter One Access Control Policy. Providing access to another individual, either deliberately or through failure to secure a device is prohibited.

All end-user, personal or company-owned devices used to access company information systems (i.e. email, chat applications (ex: Slack, Teams, etc.), Google services, etc.) or data must adhere to the following rules and requirements:

- Devices must be locked with a password (or equivalent control such as biometric) protected screensaver or screen lock after no more than 10 minutes of non-use.
- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a device immediately to the IT Manager
- Confidential information must not be stored on devices or USB drives; "stored" in this context does not mean accessed via mobile apps.
- All working documents should be saved on the shared company Google Drive. Downloads should be deleted immediately after use.
- Any device used to access company resources (such as file shares and email) must

- not be shared with any other person
- Upon termination, users agree to return all company-owned devices and delete all company information and accounts from any personal devices

7. Use of Personal Devices

Chapter One permits the use of a personal device only when company-provided equipment is not functioning or accessible.

This option can be particularly useful on the rare occasions when IT staff are unavailable and Chapter One equipment is not functioning correctly. It allows staff to continue day-to-day work without interruption, while they wait for IT team assistance.

The IT team is able to provide instructions about how to access Google accounts if needed.

If a personal device is used for a limited, emergency period is critical that the following conditions are adhered to:

- This option should only be used when a company-provided device is unavailable.
- Users should aim to use incognito browser windows or private browsing mode
- Under no circumstances should any company documentation, or information be downloaded, saved, or stored on any personal device.
- Users must sign out of any Chapter One accounts after use.

8. Security of Home/Remote Devices

The nature of much of Chapter One's work means that staff normally work from home. Employees working from home should check the arrangement with their home insurance provider to ensure that any equipment which facilitates home working is covered and, if applicable, take out an appropriate policy to cover any additional risks. Chapter One cannot accept liability for damage caused to the home or its contents, nor can it meet any additional costs of insurance or pay any additional lighting or heating costs etc.

Where passwords are issued to control entry to computer systems or programs, including e-mail, these must not be shared with or made available to other members of staff, or persons not employed by Chapter One.

Working outside of an office makes Chapter One's data less secure. Employees are therefore expected to ensure that all Chapter One information is appropriately protected. This includes:

- Not keeping/saving electronic files relating to Chapter One work on any computer not under Chapter One's control. All working documents should be saved on the shared Google Drive. Downloads should be deleted immediately after use.
- When working from a home network, ensure that the default wifi settings are changed, such as name, password, and admin access.
- Ensuring that the PC being used has up-to-date virus protection and firewalls to prevent malicious or accidental corruption or disclosure of confidential data. We ask that all staff leave their laptops on overnight one day a week (currently Monday) to receive these essential updates

- On company-owned or issued computers, users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access company resources
- When it is absolutely essential to use portable storage devices to transport electronic files, this should be agreed with your Line Manager, and the IT Management Team to ensure files are kept securely, and preferably on your person at all times
- Two-factor authentication is required for remote system access. Two-factor authentication (2FA) is required for all remote system access.
- Each staff member is issued a Yubikey hardware security key as their mandatory second authentication factor. This physical security key must be inserted into a USB port and physically touched to verify the user's identity when accessing company systems remotely. All staff members must complete Yubikey setup and testing with the IT team during induction before being granted remote access permissions. Additional 2FA is in place for staff Google accounts.

9. Clear Screen Clear Desk Policy

Users shall not leave confidential materials unsecured on their desk or workspace and will ensure that screens are locked when not in use, especially in any public areas.

10. E-mail Use

Chapter One's e-mail accounts are intended to promote effective communication within the organisation on matters relating to business. The e-mail system should be used for that purpose. Brief, occasional personal messages may be sent but employees should adhere to the primary purpose of the system.

E-mail communications tend to be more informal than written correspondence, but should be treated as equivalent to letters. Pay attention to tone: hasty messages sent without proper consideration can cause upset, concern or misunderstanding. Appropriate standards are to be maintained, which should be based on common sense, reasonableness and the professional standards expected from all users by Chapter One.

E-mails sent externally are no different to letters sent out on Chapter One's headed paper, and should be treated in the same regard. Any inappropriate use of the e-mail and internet facility may result in disciplinary action up to and including summary dismissal (i.e. dismissal without notice).

"Inappropriate" includes (but is not limited to):

- any communication that might bring the professional reputation of Chapter One into disrepute, including sharing protected copyright material;
- the sending of chain letters, junk mail, advertisements other than those which are sent in the course of your duties under your contract of employment, or other trivial content including jokes, quizzes and video clips;
- sending abusive material in any e-mail whether business or personal. Examples are e-mails whose content contains any material in any of the following categories:

* defamatory;

- * offensive or obscene;
- * untrue or malicious;
- * abusive;
- * racist or sexist;
- * pornographic;
- * can otherwise be defined as harassment

Improper statements contained in e-mails may result in legal action against the member of staff or Chapter One. It is therefore vital for e-mail messages to be treated like any other form of correspondence and, where necessary, hard copies to be retained. Employees are reminded that e-mail messages (like any form of recorded material) are disclosable in any legal action commenced against Chapter One relevant to the issues set out in the e-mail.

E-mails do not always reach their destination. If a message is important, employees should make sure they obtain confirmation of receipt. Confidential information should not be sent externally by e-mail or unprotected over the internet. Chapter One is unable to guarantee the security of e-mails when sent over a public network such as the internet.

Employees must not mask or alter their identity as it appears in an e-mail header (this is known as "spoofing").

Unless an employee is specifically authorised to do so by their line manager, under no circumstances may they enter into a contractual commitment by e-mail. Please note that offers or contracts transmitted by e-mail are as legally binding to the Charity as those sent on paper.

If an employee receives an e-mail message that has been wrongly delivered to their e-mail address, they should notify the sender of the message by redirecting the message to that person. In the event the e-mail message contains confidential information, the employee must not disclose or use that confidential information.

Chapter One reserves the right to monitor all e-mail/internet activity by staff for the purposes of ensuring compliance with its policies and procedures and of ensuring compliance with the relevant regulatory requirements and employees hereby consent to such monitoring. This includes monitoring of any additional accounts they may be requested to set up for the purposes of performing their work tasks, which are subject to the same rules as their work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

11. Internet Use

Employees will have access to the internet for the purpose of performing their roles effectively. Guidance on the use of social media is covered in Chapter One's Social Media Policy.

We permit the incidental personal use of Chapter One systems and devices, including for example to browse the internet or send personal emails/make personal telephone calls. Personal use must not be overused, abused, or excessive, and at all times must comply with

this Policy. We may withdraw permission for it at any time or restrict access to Chapter One devices at our discretion.

At all times, the websites visited from any company equipment may be monitored. Employees are not permitted to access inappropriate websites or download offensive, obscene or indecent material. Please note that a cookie may be left on a site visited by you, and your page visits may be traceable to Chapter One and may bring the organisation into disrepute. The company monitors website activities for use and abuse of its name, logo or image.

Any information posted online about Chapter One, whether written during work or personal time, must not breach our confidentiality or data protection policies.

You must never access, or download, any unauthorised or inappropriate material, content or software. If downloading and installing software ensure it is Chapter One approved and from online sources you trust.

The ability to connect with a specific website does not in itself imply that users of the Chapter One systems are permitted to visit that site. Chapter One, may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation.

Employees must not publicly disclose internal Chapter One information through the Internet that may adversely affect trading, customer relations, or public image. Only company authorised material should be published on the Chapter One website.

Failure to comply with these provisions will result in disciplinary action up to and including dismissal.

12. Further Unacceptable Use

It's important to note that using company-owned resources or representing the company in any way to engage in activities that are illegal is strictly prohibited. The following list is not all-inclusive but aims to outline the types of activities that are considered unacceptable use over and above the sections above that relate to Email and Internet usage.

The following activities are strictly prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license
- Accessing company data, a server, or an account for any purpose other than conducting company business, even if you have authorized access, is prohibited
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The

appropriate management shall be consulted prior to the export of any material that is in question

- Introduction of malicious programs into the company network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
- Making fraudulent offers of products, items, or services originating from any company account
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties
- Effecting security breaches or disruptions of network communication. Security breaches include but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
- Port scanning or security scanning is expressly prohibited unless prior notification to the company engineering team is made
- Executing any form of company network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty and/or is approved prior to doing it.
- Circumventing user authentication or security of any company host, network, or account
- Introducing honeypots, honeynets, or similar technology on the company network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
- Providing information about, or lists of company employees, contractors, partners, or customers to parties outside the company without authorization
- Using removable media to export or store company or customer data

13. Backup and Remote Access

The use of the company's cloud-based document storage service (Google Drive) for business file storage is required for users of laptops or company-issued devices. Storing important documents on the file share is how you "backup" your laptop.

For security and network maintenance purposes, authorised individuals within the company may monitor equipment, systems, and network traffic at any time.

The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

14. Data retention and deletion

Chapter One has a data retention policy in place, as well as records of processing which set out how long data should be kept for, depending on the processing activity. Please see the Data Management Policy.

15. Information Security Awareness, Education & Training

All employees and contractors with administrative or privileged technical access to Company production systems and networks shall complete GDPR and Information Security awareness training at the time of hire and annually thereafter. Employees and contractors shall be aware of relevant information security and data privacy policies and procedures. The company shall ensure that personnel receive security and data privacy training appropriate to their role and data handling responsibilities.

In order to maintain a robust level of security awareness, the company will provide security-related updates and communications to company personnel on an ongoing basis through multiple communication channels as needed.

Information security leaders and managers shall ensure appropriate professional development occurs

16. Policy Compliance

The company will measure and verify compliance with this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits. Policies will be reviewed on a regular basis

17. Exceptions

Exceptions to this policy must follow the formal exceptions process, which requires a technical risk assessment from the Security Delegate and final approval and risk acceptance from the Chapter One UK CEO (Accountable Owner). All exceptions are logged in the Chapter One UK Exceptions Register.

18. Violations & Enforcement

Any known violations of this policy should be reported to the Security Delegate. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Change Record:

Date of Change:	Changed By:	Comments:
Nov 2025		Policy created and approved by Board