

Chapter One - Data Management and Retention Policy

1. Purpose and Scope

Purpose: to provide a high-level overview of how data is managed within Chapter One, explaining how it is classified, protected, retained and securely disposed of.

Scope: all company data, information, and information systems.

2. Policy

The classification of data and information systems is done in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

3. Data Protection Principles

Chapter One applies the Seven GDPR Data Protection Principles when processing personal data:

- **Lawfulness, fairness and transparency:** personal data will be processed fairly and lawfully.
- **Purpose limitation:** personal data will be obtained only for the purpose specified.
- **Data minimisation:** personal data kept will be adequate, relevant and not excessive for the purposes required.
- **Accuracy:** personal data shall be accurate.
- **Storage Limitation:** personal data will not be kept for longer than is necessary for purpose.
- **Integrity and Confidentiality:** personal data will be processed in accordance with the rights of data subjects.
- **Accountability:** appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

Furthermore, personal data will not be transferred outside the UK/EEA unless that country or territory ensures an adequate level of data protection for the rights and

freedoms of data subjects, except where consent is given, or where other contractual safeguards have been implemented.

4. Linked Policies

This policy must be read in conjunction with the following three policies which detail how Chapter One meets its requirements under GDPR when it handles employee, volunteer and pupil data.

- Chapter One Privacy & Data Protocols Policy for Staff
- Chapter One Privacy & Data Protocols Policy for Volunteers
- Chapter One Privacy & Data Protocols Policy for Schools

5. Data Classification

To help employees and stakeholders easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential

Highly sensitive data, or confidential data, requires the highest levels of protection; access is restricted to specific employees or departments. The handling of this data is covered by specific linked policies, as above. Example include:

- Volunteer and student Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary and payroll information
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code
- Litigation data

Restricted

Company proprietary information requires thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is the default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Strategic and business plans
- Meeting minutes and internal presentations
- Contracts

- Internal reports
- Slack messages
- Email

Public

Documents intended for public consumption can be freely distributed outside the company. Examples include:

- Marketing materials
- Product descriptions
- External facing policies

6. Labeling Paper

Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.

7. Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access is restricted to specific employees, roles, and/or departments
- Access for non-preapproved roles requires documented approval from the CEO or Head of Finance and is granted on an as-needed basis.
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall be handled like Company confidential data.
- Confidential data shall be encrypted at rest and in transit over public networks in accordance with the Cryptography Policy
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted. Mobile devices storing or accessing confidential data shall be protected by a log-on password (or equivalent, such as biometric) or passcode and shall be configured to lock the screen after ten (10) minutes of non-use
- Backups of Confidential data shall be encrypted
- Confidential data shall not be stored on removable media including USB drives, CDs, or DVDs Paper records shall be labeled "confidential" and securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures Hardcopy paper records of Confidential data shall only be created based on a business need and shall be avoided whenever possible
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement or as mandated by law or regulation, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed of in a secure, approved manner in accordance with data handling and destruction policies and procedures
- Restricted data shall not be stored on removable media including USB drives, CDs, or DVDs

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed.

8. Data Storage and Transfer

In order to maintain our services, we may store or transfer the data to affiliates or trusted third party recipients in the United States of America. This includes our affiliated organisation, Chapter One NFP with which data is shared under the protection of a data sharing agreement that incorporates the UK Addendum to the European Commission approved Standard Contractual Clauses (SCC). We may also share an administrative Google Drive account with Chapter One NFP which uses data storage facilities in the USA. These transfers are also subject to the SCCs.

Chapter One's database storage is managed by Heroku, which is based in the USA. Heroku is owned by a company called Salesforce which ensures data privacy as explained in its Data Processing Addendum (DPA) and this FAQ document. The basis for these transfers is in Salesforce's approved Processor Binding Corporate Rules and the SCCs.

Chapter One has conducted a Data Protection Impact Assessment and Transfer Impact Assessment to satisfy itself that such transfers of personal data to the USA are lawful and that the data transferred is adequately protected.

9. Data Retention

Company shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived.

Personally identifiable information (PII) shall be deleted or de-identified when it no longer has a business use. Retention periods shall be documented in the Data Retention Matrix in Appendix A to this policy.

10. Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. The organisation shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third parties who meet company requirements for secure data disposal shall be used for the storage and processing of restricted or confidential data.

Where feasible, all restricted and confidential data will be securely deleted from company devices prior to, or at the time of disposal. Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method.

11. 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.

12. 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

APPENDIX A - Data Retention Matrix

System Application or	Data Description	Retention Period
Governance	Lists of Directors and annual accounts	7 years
HR	Recruitment records	6 months
HR	Staff records	6 years after date of departure
Platform database	Volunteer PII	5 years
Platform database	Student PII	5 years
DBS Risk Assessments	Volunteer PII	2 years
Safeguarding records	Student PII	6 years
Finance and Accounting	Business and accounting records	6 years
Company Support	Customer instance and metadata, debugging data	Indefinite
Company Customer Support Tickets	Support Tickets and Cases	Indefinite
Company Security Event Data	Security and system event and log data, network data flow logs	Cloud/Host Instance - 1 year
Company Vulnerability Scan Data	Vulnerability scan results and detection data	6 months - host (asset) data is retained until removed and purged from the vulnerability management tool
Company QA and Testing Data	QA, testing scenarios, and results data	Indefinite
Security Policies	Security Policies	1 year after archive
Temporary Files	IaaS /tmp ephemeral storage	automatically when the process finishes