Record Retention Policy

Policy Scope

This policy covers all directors, employees, contractors, visitors and subsidiaries of the Confederation of School Trusts (the Group), setting out the standards and limitations the Group applies regarding the classification to members, clients, customers, users, non-members (Service Users) and employees data records. It provides a framework to ensure that the data protection obligations are met concerning the retention and disposal of Service Users and employee data. Subsidiary companies include CST Professional Development Limited (Company number 10354936).

'Principle e' in Article 5 of the United Kingdom General Data Protection Regulation (UK GDPR) states that 'personal data must not be kept longer than is necessary for the purposes for which the personal data are processed'.

The Group only retain personal data for as long as necessary to fulfil the identified business purpose for which the data was collected and according to the retention schedule period as set out in the Record Retention Schedule.

Policy

We operate a paperless office, and unless a specific request has been made for a hard copy document, all records are to be stored electronically using SharePoint, Teams or the CRM system.

Where hard copy documents are required, they shall be stored in a dry and secure location to prevent loss or deterioration, and stored in a manner that is legible, readily identifiable and appropriately retrievable.

Retention periods, where consider both statutory and customer requirements, are shown in the Record Retention Schedule, which is an essential component of an efficient records management system. This protects the interests of the Group and its Service Users by ensuring records are kept only for as long as they are needed, to meet operational needs, comply with legal and regulatory requirements, and are then disposed of securely.

The Record Retention Schedule evidences the retention period for the different record classifications and respective trigger which starts any retention period.

Where it is not possible to define a statutory or legal retention period, as per the UK GDPR requirement, we provide this to data subjects on request and in consideration of the published privacy notice.

Report Retention Protocols

All Service User data held by the Group is retained, stored, and destroyed in line with legislative and regulatory obligations. The Group recognises that by managing records correctly, it supports core functions and helps us to comply with legal and regulatory obligations. We are committed to the efficient management of our records, for the effective delivery of services. The benefits of effective records management are:

- Protecting business critical records and improving business resilience;
- Ensuring information can be found and retrieved quickly and efficiently;
- Complying with legal and regulatory requirements;
- Reducing risk through audits and reviews; and
- Minimising storage requirements and associated costs.

To assist with the above, the Group undertake the following:

- Carry out periodical audits of retained data, checking purposes, continued validity, accuracy and requirement to retain;
- Establish periodical reviews of data retained; and
- Establish and verify retention periods of data with consideration of:
    - The operational requirements of the Group or subsidiary
    - The type of personal data
    - The purpose and lawful basis for processing
    - The categories of data subjects

Where it is not possible to define a statutory or legal retention period, as per the UK GDPR requirements, we provide this to data subjects on request and in consideration of the published privacy notice. We would not typically retain paper records for longer than seven years.

Definitions

Personally Identifiable Information (PII) - is any data that can be used to identify an individual. This includes both direct identifiers like a name or National Insurance number, and indirect identifiers

such as a combination of name, birth date, and other personal detail, email addresses, phone numbers, and bank account numbers.

Categories of Personal Data – to determine whether you are processing personal data, consider:

- identifiability and related factors;
- whether someone is directly identifiable;
- whether someone is indirectly identifiable;
- the meaning of 'relates to'; and
- when different organisations are using the same data for different purposes.

Special Categories of Personal Data - some of the personal data processed can be more sensitive in nature and therefore requires a higher level of protection. The UK GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Record Retention Schedule

All information assets are assigned an owner, who is responsible for those assets produced and stored within each department, and has agreed with the retention periods noted in the Record Retention Schedule. Information Asset Owners are responsible for ensuring that retention periods are regularly reviewed, at least annually, to ensure they remain appropriate.

The Record Retention Schedule includes the following information:

1) **Legal Entity**: the legal entity that the records pertain to;
2) **Department**: the department that holds these records;

3) **Information Asset Type**: the type of data record held;
4) **Relevant UK Legislation**: primary legislation with a direct bearing on the retention period;
5) **GDPR**: principles that apply to the asset type;
6) **Retention Period**: the recommended length of time for which an asset should be kept. The retention period is often expressed as a starting point, plus an additional year, to aid in the final disposal action;
7) **Information Asset Owner**: owner responsible for the asset and implementation / update of their section of the Record Retention Schedule;
8) **ROPA Ref**: the cross reference to the entry in the Record of Processing Activities (ROPA);

ROPA

The ROPA is the Group's record of processing activities. The Group is not required under Article 30 if the UK GDPR to maintain a ROPA, however we recognise that this is good practice.

The Group only keeps personal information for as long as needed to meet the business requirements for which the information was collected.

The ROPA contains the following information against each processing activity:

1) Process Name
2) Responsible Person
3) Our Role: this contains the type of role undertaken by the Group the choices are:
    - PII Controller - determines the purposes and means for processing personally identifiable information (PII), responsible for the implementation of privacy and security protocols to meet applicable legal standards.
    - PII Joint Controller – is two of more entities who determines the purpose and means for processing PII (see PII Controller).
    - PII Processor - processes personal data on behalf of the controller.
4) Business Function
5) Department
6) Purpose of processing: description of what the purpose of holding the information is for.
7) Categories of individuals: type of individual for example suppliers, clients, business, employees etc

8) Categories of Personal Data: this should contain the type of data held, for example client name, company address, company email, company telephone number, bank details, date of birth
9) Special Categories of Personal Data or Criminal Data
10) Categories of External Recipients: type of recipients receiving information
11) Legal Basis for Processing: taken from Article 6 GDPR
12) Names of third countries/ international organisations that personal data are transferred to: to understand where the information is going to so that appropriate safeguards and agreements are in place to protect the data.
13) International Transfer Safeguards: list safeguard type, DPIA, TRA, Data Privacy Framework registration
14) Retention Schedule: period of time information will be kept for before deletion
15) General description of technical and organisational security measures: description of transfer of the information for example through secure system, email, teams link etc

All Information Assets are assigned an owner, who is responsible for those assets produced and stored within each department and has agreed the retention periods noted in the Record Retention Schedule. Asset owners are responsible for ensuring that retention periods are regularly reviewed, at least annually, to ensure they remain appropriate.

Disposal of Records

Records will not be destroyed of without the authorisation of the individual responsible for their retention and disposal.

Records to be destroyed are to be destroyed in a controlled manner. Electronic copies will be deleted using appropriate software and hard copies destroyed through confidential waste disposal including appropriate level shredding.

Regulatory Requirements

We must ensure compliance with all applicable laws and regulations in the jurisdiction in which we operate. Policies and controls must be designed, as a minimum, to ensure compliance with local laws, regulations, and best practice.

All staff must ensure compliance with the Data protection Act 2018/ UK GDPR and all applicable laws and regulations in the jurisdiction in which we operate. Policies and controls must be designed to ensure compliance with local laws, regulations and best practice.

Compliance

Exceptions to this policy must be approved by the Chief Operating Officer in writing.

All breaches of this policy, actual or suspected must be reported to your line manager initially. In certain cases, the incident may be raised with the IT department and the Information Security Team who will ensure it is investigated. Breaches of this policy may be considered as gross misconduct, and in certain cases lead to termination of employment and/or legal action/prosecution.

The default review frequency position is 12 months, however a review may be required sooner depending on the nature of the Policy

Appendix – Procedure for Auditing Record Retention

Reference to "auditor" can include an internal member of staff or external consultants undertaking reviews and audits on behalf of the Group.

- The auditor should examine the Record Retention Schedule and select a sample of four processes for auditing.
- The auditor should then meet with the department responsible for each process selected and the selected records should be examined to ensure that they comply with the retention period stated in the Record Retention Schedule.
- The auditor will then compile a report stating which processes have been audited and whether the records comply with the stated retention period.
- The Record Retention Audit Report should be forwarded to the Chief Operating Officer for their review.
- The Chief Operating Officer will sign off the report and make recommendations as required.
- All reports containing recommendations will be submitted to the Governance and Compliance Committee.