2025

Policy: Data Protection, Retention and Privacy

SRSCC

Skills Training Apprenticeships

OWNER: CEO

SR Supply Chain Consultants Limited | Parkside House, 190-192 Wigan Road, Euxton, Chorley,
Lancashire, PR7 6JW

Last Review Date:	14/11/2025
Next Review Date:	14/11/2026
Author:	Susan Rashid
Signed:	
Position:	CEO
Approved by:	Eileen Moran
Signed:	
Position:	Quality and Compliance Manager

Contents

Policy Summary

SRSCC is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out SRSCC's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, apprentices, and former employees, referred to as HR-related personal data.

SRSCC has appointed Susan Rashid (CEO) as the person with responsibility for data protection compliance. They can be contacted at susan.rashid@srscc.co.uk. Questions about this policy, or requests for further information, should be directed to them.

SRSCC Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Aims and Objectives

Data Protection Law

The Data Protection Act 2018 describes how organisations — including SRSCC, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

SRSCC processes HR-related personal data in accordance with the following data protection principles:

- SRSCC processes personal data lawfully, fairly and in a transparent manner.
- SRSCC collects personal data only for specified, explicit and legitimate purposes.
- SRSCC processes personal data only where it is adequate, relevant, and limited to what is necessary for the purposes of processing.
- SRSCC keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- SRSCC keeps personal data only for the period necessary for processing.

- SRSCC adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction, or damage.

This data protection policy ensures SRSCC:

- Complies with the Data Protection Act 2018 and follow good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Commitment

At SRSCC, we are dedicated to upholding the highest standards of quality and ensuring the effective implementation of the following policy:

We commit ourselves to the principles, goals, and objectives set forth in this policy, and we will actively work towards its successful implementation. As an organisation, we recognise the importance of aligning our actions with the policy's provisions to achieve the desired outcomes. Our commitment includes:

- Compliance: We will diligently adhere to all the guidelines, procedures, and regulations outlined in the policy. We will ensure that our actions are consistent with the intended spirit and objectives of the policy.
- Responsibility: We acknowledge our roles and responsibilities in implementing the policy. Each member of our organisation will be aware of their specific duties and contribute to the successful execution of the policy.
- Resources: We will allocate the necessary resources, to support the implementation of the policy. We understand that adequate resources are essential for its effective execution.
- Timelines: We will establish clear timelines and milestones to ensure timely progress towards the policy's objectives. We will regularly review and assess our progress to stay on track and make adjustments as needed.

- Reporting and Monitoring: We will establish robust reporting and monitoring mechanisms to track our performance and measure the outcomes of the policy. We will provide timely and accurate reports to relevant regulatory bodies and internal teams as required.
- Continuous Improvement: We are committed to continuously improving our processes, systems, and practices to enhance the effectiveness of the policy's implementation. We will actively seek feedback, identify areas for improvement, and implement necessary changes to achieve better results.
- Training and Awareness: We will invest in training programmes and initiatives to ensure that all our staff members are aware of the policy, its objectives, and their individual responsibilities. We will foster a culture of awareness and understanding to promote policy adherence throughout the organisation.

We recognise that upholding the quality and successful implementation of this policy requires the collective effort and commitment of every individual within our organisation. By adhering to this commitment statement, we aim to create a culture of excellence, accountability, and continuous improvement.

Terms of Reference

Personal data - is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.

Special categories of personal data - means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

Criminal records data - means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Scope

This policy applies to:

- The head office of SRSCC
- All study centres of SRSCC

- All staff and associates of SRSCC
- All contractors, suppliers and other people working on behalf of SRSCC

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Date of birth
- Any other information relating to individuals

Responsibilities

Responsibilities	Details
CEO	- Ultimately responsible for ensuring that SRSCC meets its legal obligations
Head of Central Services	- Keeping the CEO updated about data protection responsibilities, risks and issues. - Reviewing all data protection procedures and related policies, in line with an agreed schedule - Arranging data protection training and advice for the people covered by this policy. - Handling data protection questions from staff and anyone else covered by this policy. - Dealing with requests from individuals to see the data - SRSCC holds about them (also called ‘subject access requests’) - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data
IT Support Officer	- Ensuring all systems, services and equipment used for storing data meet acceptable security standards. - Performing regular checks and scans to ensure security hardware and software is functioning properly. - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services
Marketing Manager	- Approving any data protection statements attached to communications such as emails and letters.

	- Addressing any data protection queries from journalists or media outlets like newspapers. - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

Process Overview

SRSCC informs individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where SRSCC relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where SRSCC processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Data and Data Protection Risks

This policy helps to protect SRSCC from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Use of Artificial Intelligence (AI)

Where AI tools process personal data, the Company will ensure transparency, lawful basis for processing, and the ability for individuals to exercise their rights regarding automated decision-making.

Data/Information Classification

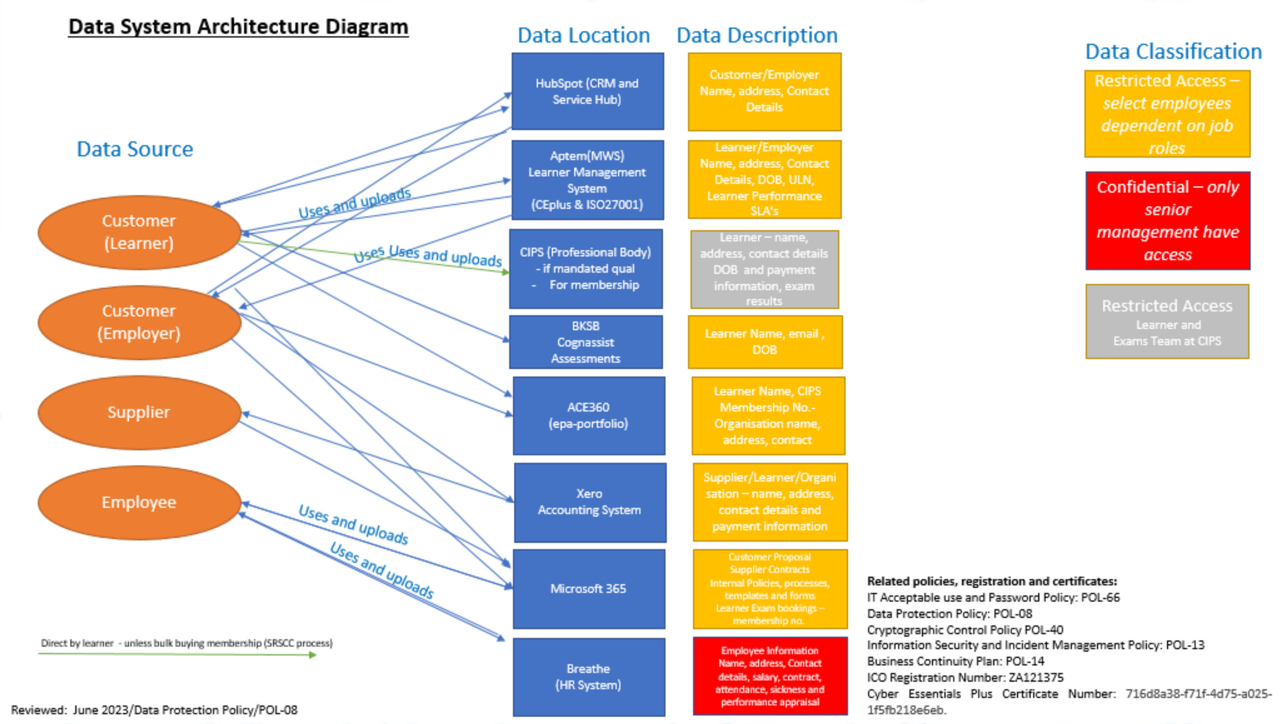
SRSCC assesses and classifies the data held and level of protection that should be given.

Information held at SRSCC is classified in terms of confidentiality as follows:

1. Confidential (only senior management have access)
2. Restricted (most employees have access)
3. Internal (all employees have access)
4. Public information (everyone has access)

Data Source	Description of Data	Data Classification	Data Location
Customer	Employer Name, Address, Contact Details	Restricted	Aptem E-portfolio, Hubspot (CRM), Xero (accounting)
Customer	Learner Names, Address, Contact Details, DOB, ULN	Restricted	Aptem E-Portfolio, ILR, ACE360/EPA Pro
Customer	Employer Contracts	Restricted	MS Teams & Aptem E-Portfolio
Customer	Learner Performance Records	Restricted	Aptem E-Portfolio
Employee	Name, Address, Contact Details	Confidential	Breathe
Employee	Salary and Contract	Confidential	Breathe
Employee	Attendance, sickness, and performance appraisals	Confidential	Breathe
Supplier	Names, address, contracts, payment information	Restricted	Xero and MS Teams
Policies	Master Policies	Internal & Public	MS Teams/Website
Templates	Forms and Templates	Internal	MS Teams

Data System Architecture Diagram


Data System Architecture Diagram
Data Source
Customer (Learner)
Customer (Employer)
Supplier
Employee
Uses and uploads
Uses Uses and uploads
Uses and uploads
Uses and uploads
Data Location
HubSpot (CRM and Service Hub)
Aptem(MWS) Learner Management System (CEplus & ISO27001)
CIPS (Professional Body) - if mandated qual - For membership
BKSB Cognassist Assessments
ACE360 (epa-portfolio)
Xero Accounting System
Microsoft 365
Breathe (HR System)
Data Description
Customer/Employer Name, address, Contact Details
Learner/Employer Name, address, Contact Details, DOB, ULN, Learner Performance SLA's
Learner – name, address, contact details DOB and payment information, exam results
Learner Name, email , DOB
Learner Name, CIPS Membership No.- Organisation name, address, contact
Supplier/Learner/Organisation – name, address, contact details and payment information
Customer Proposal Supplier Contracts Internal Policies, processes, templates and forms Learner Exam bookings – membership no.
Employee Information Name, address, Contact details, salary, contract, attendance, sickness and performance appraisal
Data Classification
Restricted Access – select employees dependent on job roles
Confidential – only senior management have access
Restricted Access Learner and Exams Team at CIPS
Direct by learner - unless bulk buying membership (SRSCC process)

Related policies, registration and certificates:
IT Acceptable use and Password Policy: POL-66
Data Protection Policy: POL-08
Cryptographic Control Policy POL-40
Information Security and Incident Management Policy: POL-13
Business Continuity Plan: POL-14
ICO Registration Number: ZA121375
Cyber Essentials Plus Certificate Number: 716d8a38-f71f-4d75-a025-1f5fb218e6eb.

Reviewed: June 2023/Data Protection Policy/POL-08

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.

Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures PRO-151 Data Backup Procedures.docx..

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

Personal data is of no value to SRSCC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires SRSCC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort SRSCC should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

- Files downloaded must be moved out of the downloads folder by the end of each day and the empty folder must be reviewed at the beginning of the following day.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- SRSCC will make it **easy for data subjects to update the information** SRSCC holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Data Security

SRSCC takes the security of HR-related personal data seriously. SRSCC has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure and to ensure that data is not accessed, except by employees in the proper performance of their duties. Please refer to the Information Security and Incident Management Policy for further information.

Where SRSCC engages third parties to process personal data on its behalf, such parties will do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Impact Assessments

Some of the processing that SRSCC carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, SRSCC will carry out a data protection impact assessment (DPIA) to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

If SRSCC Ltd discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. SRSCC will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with ***information.***

Individual Rights

As a data subject, individuals have several rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, SRSCC will inform the individual:

- Whether or not their data is processed, and if so why, including the categories of personal data concerned and the source of the data if it is not collected from the individual.
- To whom their data has or may be disclosed to, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- For how long their personal data is stored (or how that period is decided).
- Their rights to rectification or erasure of data, or to restrict or object to processing.
- Their right to complain to the Information Commissioner if they think SRSCC has failed to comply with their data protection rights; and
- Whether or not SRSCC carries out automated decision-making, and the logic involved in any such decision-making.

SRSCC will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically unless the individual agrees otherwise.

To make a subject access request, the individual should send the request to susan.rashid@srscc.co.uk. In some cases, SRSCC may need to ask for proof of identification before the request can be processed. SRSCC will inform the individual if it needs to verify their identity and the documents it requires.

SRSCC will normally respond to a request within a period of one month from the date it is received. In some cases, such as where SRSCC processes large amounts of the individual's data, it may respond within three months of the date the request is received. SRSCC will write to the individual within one month of receiving the original request to advise if this is the case.

If a subject access request is manifestly unfounded or excessive, SR Supply Chain Consultants Ltd is not obliged to comply with it. Alternatively, SRSCC can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which SRSCC has already responded.

If an individual submits a request that is unfounded or excessive, SRSCC will notify the individual that this is the case and whether the request will be responded to. All individuals who are the subject of personal data held by SRSCC are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**

- Be informed how the company meets **its data protection obligations**.

Other Rights

Individuals have several other rights in relation to their personal data. They can require SRSCC to:

- Rectify inaccurate data.
- Stop processing or erase data that is no longer necessary for the purposes of processing.
- Stop processing or erase data if the individual's interests override SRSCC's legitimate grounds for processing data (where SRSCC relies on its legitimate interests as a reason for processing data).
- Stop processing or erase data if processing is unlawful.
- Stop processing data for a specified period if the data is inaccurate or if there is a dispute about whether the individual's interests override SRSCC's legitimate grounds for processing data.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, SRSCC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

SRSCC aims to ensure that individuals are aware that their data is being processed, and that they understand:

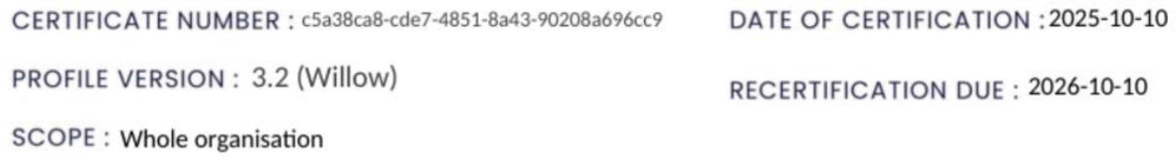
- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

Related policies, registration and certificates:

IT usage and Password Policy:	POL 66
ICO Registration Number:	ZA121375, expiry 7/6/2026

Cyber Essentials Plus Certificate Number: Expiry 10/10/26



CERTIFICATE NUMBER : c5a38ca8-cde7-4851-8a43-90208a696cc9

DATE OF CERTIFICATION : 2025-10-10

PROFILE VERSION : 3.2 (Willow)

RECERTIFICATION DUE : 2026-10-10

SCOPE : Whole organisation

https://www.cyberessentials.ncsc.gov.uk/

Privacy Notice – How we use your data

The categories of learner information that we collect, hold and share include:

- Personal information (such as name, DOB, ULN, CIPS number, address, National Insurance number, employer details, email address)
- Characteristics (such as ethnicity, language, nationality)
- Attendance information (such as session attended, number of absences and absences and reasons)
- Assessment of educational progress & outcomes, development and behaviour including that relating to special needs
- Meetings, sessions, and workshop recording

Why we collect and use this information

We use learner data:

- To support learning
- To monitor and report on learner progress.
- To provide appropriate support and care
- To assess the quality of our services
- To comply with the law regarding data sharing
- To safeguard learners
- To comply with DFE data collections requirements (apprentices only – see How DfE shares personal data - GOV.UK (www.gov.uk)
- To process learners Chartered Institute of Procurement and Supply (CIPS) membership and assessment entry.
- Marketing – we may use your contact details to provide you with information on upcoming courses, procurement and supply news, key dates and deadlines and special offers and promotions. We may use a 3rd party provider to send out these emails. You can opt out of these emails by clicking “unsubscribe” at the bottom.

The lawful basis on which we use this information

The condition for processing under the GDPR will be:

We collect and use learner information under Article 6 ad Article 9 for reasons of:

- Consent
- Necessity to perform our contract.
- Necessity to comply with DFE ILR data collection requirements.
- Necessity to enter learners for the Chartered Institute or Procurement and Supply (CIPS) assessments.

Storing learner data

We hold learner data on our cloud, Aptem, CRM and e-portfolio and potentially Xero, accounts, up until 3 years after the learner has completed their training. All servers are based in the UK and have the relevant security measures in place in the line with GDPR.

Collecting learner information

The information we collect through our registration forms is based on the requirements of the Chartered Institute of Procurement and Supply (CIPS), and in the case of apprentices, the DFE. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information or whether it is voluntary.

Who we share learner information with

We share learner information as required with the following parties:

- Chartered Institute of Procurement and Supply (CIPS)
- The Education and Skills Funding Agency (DFE)
- Department for Education (DFE)
- Ofsted
- Learner Record Service
- Chartered Management Institute (CMI)
- BKSB
- Aptem
- ACE360/epaPro
- Hubspot
- Cognassist

- E-Signature

International Data Transfers

SRSCC will not transfer HR-related personal data to countries outside the EEA.

Why we share learner information

We share learner information with on statutory basis. The data sharing is required for the awarding of the CIPS certifications and in the case of apprenticeships for the drawdown of levy funding. Please see the DFE Data Sharing policy for more information.

Individual Responsibilities

Individuals are responsible for helping SRSCC keep their personal data up to date. Individuals should let SRSCC know if data provided to them changes, for example, if an individual moves house or changes bank details, these can be updated via their BreatheHR record.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment. Where this is the case, SRSCC relies on individuals to help meet its data protection obligations to staff, customers, and clients.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes.
- Not to disclose data except to individuals (whether inside or outside SRSCC) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction).
- Not to remove personal data, or devices containing, or that can be used to access personal data, from SRSCC's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device. Please refer to the IT Acceptable Use Policy for Learners and Staff and Cryptographic Control Policy for further information.
- Not to store personal data on local drives or on personal devices that are used for work purposes.
- To report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under SRSCC's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

SRSCC will provide training to all individuals about their data protection responsibilities as part of the induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy, or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

CCTV

SRSCC operates CCTV on external areas of the premises, for the purpose of security and for crime prevention. Your image, may therefore, be captured by CCTV, but will only be accessed by an authorised manager. Your image could be shared as part of an investigation with HR, H&S advisors, Health and Safety Executive and the police. By the nature of an investigation this list is not exhaustive.

Requesting access to your data

Under the GDPR legislation, learners have the right to request access to the information we hold about them. To make a request for your personal information please contact susan.rashid@srscc.co.uk.

You have the right to:

- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.
- In certain circumstances have inaccurate personal data rectified, blocked, erased or destroyed.
- Claim compensation for damages caused by breach of GDPR regulations.
- Object to processing of personal data that is likely to cause or is causing damage or distress.

If you have a concern about the way we collect or use your personal data please raise the concern with us in the first instance. Alternatively, you can contact the Information Commissioner’s Office at https://ico.org.uk/concerns

Contact

If you would like to discuss please contact:

SRSCC Ltd

Parkside House

190-192 Wigan Road

Euxton, Chorley

Lancashire

PR7 6JW

Data Deletion/Destruction/Retention

Data destruction is the process of safely and securely destroying sensitive data. In the context of IT asset disposal, data destruction refers to the sanitisation of data contained on data-bearing devices such as hard drives, servers, hard disks, and mobile devices.

Depending on the data and where it is stored there are three methods available for secure data destruction:

Overwriting – In the process of overwriting, old files are 'overwritten' with new files. This is also known as data erasure.

Degaussing – Degaussing uses specialist hardware to erase the magnetic field contained in storage media, making it unreadable.

Physical Destruction – This process entails the physical destruction of data bearing devices through methods such as disk shredding.

Appendix A sets out schedule of data retention and recommended disposal methods.

Data Leakage Prevention

The purpose of this section is to prevent the unauthorised disclosure, transmission or extraction of personal, confidential or commercially sensitive information belonging to SR Supply Chain Consultants Ltd (SRSCC), its learners, employers, partners and employees.

This aligns with **ISO 27001:2022 Control A.8.12**, UK GDPR, the Data Protection Act 2018, and associated DFE/DfE contractual requirements.

Scope

This policy applies to:

- All employees, contractors, associates and tutors
- All systems handling SRSCC data (e.g. Aptem, SharePoint, ACE360, HubSpot, MS365, Cognassist)
- All personal data, special category data, learner information and operational data

- All devices accessing SRSCC information (company-owned or "bring your own device" (BYOD) where permitted)

Definition of Data Leakage

Data leakage is defined as:

"The unauthorised disclosure, transfer or release of sensitive information, whether deliberate or accidental, through any communication channel or storage medium."

This includes:

- Sending data to the wrong recipient
- Uploading files to non-approved systems
- External sharing of links without correct permissions
- Storing or forwarding data through personal email accounts
- Unauthorised access caused by weak security controls
- Copying data to unencrypted or unmanaged devices

Controls to Prevent Data Leakage

Technical Controls

- Use of **Microsoft 365 security controls**, including DLP (Data Loss Prevention) rules, MFA and encryption.
- Access to systems via role-based permissions following least-privilege principles.
- Encryption of data at rest and in transit across all managed systems.
- Prohibition of storing organisational data on personal devices unless authorised and protected (MFA, encryption, Mobile Device Management (MDM) policies).
- Automated blocking of external sharing when risk thresholds are met.

Organisational Controls

- Mandatory annual Data Protection Training for all staff.
- Quarterly access reviews undertaken by the Data Protection Officer (DPO) and IT Support.

- Incident reporting procedures that require staff to report any suspected data leakage within **2 hours** of discovery.
- Approved systems register maintained by SRSCC (e.g. Data Storage Locations Register).

User Behaviour Controls

- Staff must only use approved communication channels (MS Teams, official email, SharePoint).
- Prohibition of using personal email accounts, private messaging apps, or non-approved cloud storage (e.g. Dropbox, WhatsApp, personal Google Drive).
- Mandatory verification of recipients before sending personal or sensitive information.
- Strong password practices and MFA for all accounts.

Monitoring & Detection

SRSCC uses Microsoft 365 DLP, audit logs and system alerts to detect unusual data movement. Alerts are reviewed by the DPO and the IT Security Lead.

Reporting & Incident Response

Any suspected or actual data leakage must be reported immediately via:

- The Data Breach Notification Form
- Email to the DPO
- If high risk: escalation to CEO within **4 hours**

All breaches are handled in line with this policy and ICO reporting requirements.

Data Masking

Data masking ensures that personal or sensitive data is protected during processing, analysis, training, or system testing by replacing identifiable values with anonymised or pseudonymised alternatives.

This supports the principles of **data minimisation**, **privacy by design**, and **confidentiality** under UK GDPR.

When Data Masking Must Be Applied

Data masking MUST be used when:

- Providing learner or personal data to external contractors (unless strictly required and covered by contract/DPA).
- Conducting system testing or development work.
- Exporting data for reporting where identifiable detail is not needed.
- Using AI tools, analytics platforms or automation scripts.
- Sharing data internally between teams for non-essential purposes.

Methods of Data Masking

SRSCC may use the following approved methods:

Anonymisation

Removing all identifiers so data subjects cannot be identified (directly or indirectly).

Pseudonymisation

Replacing identifiers with coded references accessible only through controlled key-files.

Redaction

Removing sensitive fields entirely when they are not required.

Tokenisation

Substituting sensitive data elements with non-sensitive placeholders.

Data Minimisation

Only extracting the minimum fields required to complete the task.

Roles & Responsibilities

- **Data Protection Officer (DPO)** ensures masking standards align with GDPR and ISO27001.
- **IT Support** implements system-level data masking controls where available.
- **Managers** ensure staff follow masking protocols before sharing data.

- **All staff** are responsible for removing or masking unnecessary personal data before sharing or transferring information.

Prohibited Practices

- Sharing raw learner/employee data unless there is a documented, lawful purpose.
- Exporting or using unmasked data in AI tools unless approved by the DPO.
- Storing identifiable data in personal drives, local computer folders, or unauthorised platforms.

Appendix A

Schedule of Data Retention and Disposal Methods

This schedule sets out how long information should be retained and disposed of using:

Overwriting – In the process of overwriting, old files are ‘overwritten’ with new files. This is also known as data erasure.

Degaussing – Degaussing uses specialist hardware to erase the magnetic field contained in storage media, making it unreadable.

Physical Destruction – This process entails the physical destruction of data bearing devices through methods such as disk shredding.

Learner Records

Information Type	Format	Retention Period
Name	Electronic – Aptem	3 years or upon request
Address	Electronic – Aptem	3 years or upon request
ULN	Electronic – Aptem	3 years or upon request
DOB	Electronic – Aptem	3 years or upon request
Qualifications	Electronic – Aptem	3 years or upon request
Meeting Recordings	Electronic – Aptem	3 years or upon request
IT		
IT Business Case	Electronic	5 years
Major Incidents Reports	Electronic	7 years
Instant Messenger & Teams Private Chat	Electronic	30 days
HR		
Pay, Pension	Electronic	7 years
Appraisals and Disciplinaries	Electronic	7 years
Personal Information	Electronic	7 years
CV’s	Electronic	7 years
Certificates	Electronic	7 years

MI	Electronic	7 years
Policy Documents		
Policies	Electronic	7 years
Templates	Electronic	7 years
Documents	Electronic	7 years

Implementation

SRSCC Ltd will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment relationship is held in the individual's personnel file in electronic format on BreatheHR. Personal records are also held in the accounts system and Sage for the purposes of processing expenses and payroll. Periods for which SRSCC holds HR-related personal data are contained in its privacy notices to individuals and within the relevant HR policy.

SRSCC keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **SRSCC will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used,** and they should never be shared in line with the password policy.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of (unless a contract provides that it should be kept).

Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Monitoring and Review

At SRSCC, we understand the importance of monitoring and reviewing our policies to ensure their effectiveness and relevance. We are committed to conducting regular assessments and making necessary adjustments to achieve the desired outcomes. This Monitoring and Review Statement outlines our approach to monitoring and reviewing the Data Protection, Retention and Privacy Policy.

Monitoring

We will establish a comprehensive monitoring framework to track the implementation of the policy. This will involve regular data collection, analysis, and evaluation of key performance indicators (KPIs) related to the policy's objectives. The monitoring process will include:

- Data Collection: We will gather relevant data and information to assess the progress, impact, and compliance related to the policy.
- Analysis: We will analyse the collected data to identify trends, strengths, weaknesses, and areas for improvement. We will use this analysis to inform decision-making and guide policy adjustments, if necessary.
- Evaluation: We will evaluate the impact and effectiveness of the policy by comparing the achieved results against the desired intent and implementation.

Review

We are committed to conducting periodic reviews of the Data, Protection, Retention and Privacy Policy to ensure its ongoing relevance and alignment with organisational goals. The review process will involve:

- Review Period: Initially, the review period for this policy will be set at annually. However, we acknowledge that circumstances may change, and it may be necessary to alter the review period based on evolving needs or external factors.
- Stakeholder Involvement: We will actively involve relevant stakeholders, including employees, managers, and external experts, in the review process. Their insights and feedback will contribute to a comprehensive evaluation of the policy's performance.

- Communication: We will ensure effective communication of any policy changes resulting from the review process. This will include notifying relevant stakeholders, providing updated documentation, and facilitating necessary training or awareness initiatives while taking into consideration SRSCC's communications strategy.

By implementing a robust monitoring and review process, we aim to continuously improve the effectiveness of the Data Protection, Retention and Privacy Policy. We are committed to maintaining its relevance, ensuring compliance, and driving positive outcomes for our organisation and stakeholders.

Document Update

This section outlines any fundamental updates to this policy.

Date of Update	Update	Person Responsible
27.07.20	Policy created	Steven Hoole
27.02.23	Updated system diagram	Susan Rashid
07.03.23	Combined Employee with Employer and Learner	Susan Rashid
05.06.23	Hubspot Service Hub	Susan Rashid
16.08.23	Update Privacy notice	Susan Rashid
09.08.24	Update new third party and ICO Cert No.	Susan Rashid
20.05.25	Insert Data Backup Procedure Link	Susan Rashid
14.10.25	Use of AI	Eileen Moran
14.11.25	Data Leakage and Data Masking	Susan Rashid