Staff Confidentiality and Data Protection Policy

Document Control

Document Title	Staff Confidentiality and Data Protection Policy
Version Number	001
Status	Approved
Publication Date	18th May 2026
Policy Owner / Author	Directors
Review Date	18th May 2027
Approved / Ratified by	Directors
Distribution	All Staff, Volunteers, Directors, Sessional Workers

1. Purpose

This policy sets out the confidentiality and data protection obligations that apply to all who work for South Cumbria Skills Exchange (SCSE), operated by Whamos Training and Development CIC. It addresses confidential business information, the protection of personal data, the handling of staff personal data, and the ownership of inventions and discoveries made during the course of SCSE work.

Because SCSE delivers training, qualifications and unregistered Alternative Provision (AP) for children and young people, confidentiality obligations are central to safe practice. Learners, families, commissioning schools, awarding organisations and partners must be able to trust that information shared with SCSE will be handled responsibly.

2. Scope

This policy applies to all employees, sessional workers, volunteers and Directors. It sits alongside the wider Secure Data Handling and Data Protection Policy (which governs the organisation's data processing as a whole) and the Confidentiality Policy and Agreement (which covers learner-facing confidentiality and how concerns are escalated).

3. Confidential information

All information that:

- has been or is acquired by you during, or in the course of, your work for SCSE, or has otherwise been acquired by you in confidence;
- relates particularly to SCSE's business, or that of other persons or bodies with whom SCSE has dealings of any sort; and
- has not been made public by, or with the authority of, SCSE,

is confidential. You may not, at any time, whether before or after the termination of your employment or engagement, disclose such information to any person without SCSE's prior written consent, save in the proper course of SCSE's business or as required by law.

Examples of confidential information include but are not limited to:

- Learner records, assessments, attendance and safeguarding information.
- Information about families, commissioning schools, and partner organisations.
- Staff personal information (including pay, contracts, performance, disciplinary or grievance matters).
- Commercially sensitive information, including pricing, supplier arrangements, funder relationships, and bid material.

- Awarding body information, examination materials, and assessment evidence.
- Internal financial, operational, and governance information.

4. Care of confidential information

You are required to exercise reasonable care to keep safe all documentary or other material containing confidential information, in any format (paper, electronic, audio, image, or other).

In practical terms this includes:

- Storing paper records in lockable storage and not leaving them visible to others.
- Locking screens when leaving devices unattended.
- Not discussing confidential matters in public places where you can be overheard, including on public transport.
- Not sharing confidential information with family members or friends, even if those people would not pass the information on.
- Not posting any confidential information on social media or in any public-facing forum.
- Returning all confidential information to SCSE on the termination of your employment or engagement, or at any other time upon reasonable demand.

5. Disclosure obligations override confidentiality

The duty of confidentiality is overridden where the law, statutory guidance, or SCSE's safeguarding obligations require information to be shared. In particular:

- Where a child is at risk of significant harm, or has disclosed abuse, the Safeguarding Policy procedures apply and must take precedence.
- Where required by a court order, a regulator, or by law enforcement under a lawful warrant, information will be disclosed as required.
- Where the disclosure is a "qualifying disclosure" under the Public Interest Disclosure Act 1998, the Whistleblowing Policy applies.

If you are uncertain whether a disclosure is required or permitted, consult a Director before disclosing.

6. Data protection

SCSE processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. As an employer, SCSE is responsible for ensuring that personal data relating to staff is processed in accordance with the data protection principles: lawfully, fairly, transparently, for specified purposes, in a way that is adequate and relevant, accurately, no longer than necessary, and securely.

The detail of how SCSE processes data — including data subject rights, retention periods, and lawful bases — is set out in the Secure Data Handling and Data Protection Policy and in the relevant privacy notices (for job applicants, employees, learners, and parents/carers).

7. Your responsibilities as a member of staff handling data

You are required to:

- Comply with all SCSE policies and procedures relating to data protection.
- Only access personal data where this is necessary for your role.
- Not transfer personal data to personal devices, personal email accounts, or unapproved cloud storage.
- Use SCSE's authorised systems and platforms (including CS Learner) for storing learner records.
- Use strong, unique passwords and protect them.
- Report any suspected personal data breach to a Director without delay so that the 72-hour reporting obligation to the Information Commissioner's Office can be met where applicable.

Failure to comply with data protection responsibilities may result in disciplinary action up to and including dismissal under the Disciplinary and Grievance Policy.

8. Your rights in relation to your own personal data

As a member of staff, you also have rights under UK GDPR in relation to the personal data SCSE holds about you. These include the right to:

- Be informed about what data SCSE holds about you and why.
- Access that data.
- Have inaccurate data corrected.
- Have data erased in some circumstances.
- Restrict or object to processing in some circumstances.
- Data portability in some circumstances.

To exercise any of these rights, contact a Director. SCSE will respond within the statutory timescales.

Where SCSE processes special category data about you (for example, health data needed for occupational health, or equality monitoring data), you will be informed and, where the lawful basis is consent, you may withhold or withdraw that consent without detriment.

9. Inventions and discoveries

An invention or discovery made by you will normally belong to you. However, an invention or discovery made by you will become SCSE's property if it was made:

- in the course of your normal duties under such circumstances that an invention might reasonably be expected to result from those duties;
- outside the course of your normal duties, but during duties specifically assigned to you, when an invention might reasonably be expected to result from these; or
- during the course of any of your duties, and at the time you had a special obligation to further SCSE's interests arising from the nature of those duties and your particular responsibilities.

If you believe you have made an invention or discovery that may fall under this section, raise it promptly with a Director so that ownership and any further steps can be discussed.

The treatment of teaching materials, training resources, lesson plans, schemes of work, photographs, and footage produced through SCSE work is governed by the Staff Code of Conduct (Section 7) and remains SCSE's property and copyright.

10. Breach of this policy

Breach of any part of this policy may result in action under the Disciplinary and Grievance Policy. Serious breaches — for example, disclosure of safeguarding information that exposes a child to risk, theft of personal data, or repeated negligence in data handling — may amount to gross misconduct.

11. Continuing obligations after employment ends

The confidentiality obligations in this policy continue after the end of your employment or engagement with SCSE. Returning SCSE property and confidential information is covered in the End of Employment Policy.

12. Related policies

This policy should be read alongside:

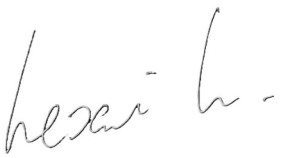
- Secure Data Handling and Data Protection Policy
- Confidentiality Policy and Agreement
- Safeguarding Policy
- Whistleblowing Policy
- Acceptable Use Policy
- Staff Code of Conduct
- End of Employment Policy
- Disciplinary and Grievance Policy

13. Policy review

This policy is reviewed annually by the Directors, or sooner in response to any change in legislation, statutory guidance, or significant operational learning.

Approval & Review

This policy has been approved on behalf of the Directors:

Elizabeth Amos-Milburn *Co-Director*	**Alexandra Gager-Liebhart** *Co-Director*
	

Date of approval: 18th May 2026

Next review: 18th May 2027

Schedule 1 — Record of Changes

Version	Date	Nature of Change
001	18th May 2026	Initial published version included in the Combined Policies and Procedures 2026 edition.