Acceptable Use Policy

Document Control

Document Title	Acceptable Use 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 Acceptable Use Policy outlines the expectations and responsibilities for all users of the systems, networks, and resources provided by Whamos Training and Development CIC. Its goal is to ensure these resources are used safely, lawfully, and in line with our mission of inclusive education.

2. Scope

This policy applies to all learners, staff, volunteers, and third parties who access or use Whamos Training and Development CIC's systems, networks, internet, and digital tools.

3. Acceptable Use

- Use all resources for educational or work-related purposes only.
- Maintain respectful and professional communication.
- Use only your assigned accounts and credentials.
- Protect your login information and report any security breaches.
- Ensure devices used on our network are secure and virus-free.

4. Unacceptable Use

- Accessing, creating, or sharing offensive, inappropriate, or illegal content.
- Attempting to gain unauthorised access to data, accounts, or systems.
- Using our systems for personal gain or commercial activity without permission.
- Deliberately introducing malware, viruses, or harmful software.
- Misusing shared documents, discussion platforms, or collabourative tools.

5. Monitoring and Compliance

All digital activity on our systems may be monitored to ensure compliance with this policy and other safeguarding and data protection requirements. Users will be informed of monitoring procedures where applicable.

6. Consequences of Misuse

Breaches of this policy may result in: - Restricted or revoked access to systems - Disciplinary action - Termination of enrolment or employment - Referral to external authorities in cases of serious misuse

7. Review and Updates

This policy is reviewed annually or as required by changes in legislation, technology, or organisational needs.

8. Online Safety and the Route for Concerns

Online safety is part of SCSE's wider safeguarding responsibility. Anyone – staff, learner, volunteer, parent or visitor – with a concern about online behaviour, content, communication, or risk encountered in connection with SCSE's systems or activities, should raise it without delay with the Designated Safeguarding Lead (Elizabeth Amos-Milburn, elizabeth@cumbriaskills.org.uk, 07809380643) or the Deputy DSL (Alexandra Gager-Liebhart, lexie@cumbriaskills.org.uk, 07985269318).

Online concerns explicitly include: cyberbullying; receipt or sharing of sexual content (including sexting / nudes); grooming; radicalisation indicators; harmful content (eating-disorder, self-harm or suicide promotion); harassment via messaging or social media; and exposure to material that has caused distress. The DSL coordinates the response in line with the Safeguarding Policy.

SCSE filters and monitors internet activity on all organisation-provided devices in line with the Department for Education's filtering and monitoring standards. Logs are reviewed where there is a safeguarding concern. The use of personal devices on site by learners is governed by this policy and by the Learner Acceptable Use Agreement in Section 10.

9. Staff-specific provisions

The following additional provisions apply specifically to staff, sessional workers, volunteers and Directors. They sit alongside the general expectations in sections 1-8 above and the Staff Code of Conduct.

Use of SCSE computer equipment

In order to keep SCSE's systems secure and reliable, the following applies to all staff:

- The introduction of new software must first be checked and authorised by a Director before installation or general use.
- Only authorised staff have access to SCSE's computer equipment, accounts and credentials.
- Only authorised software may be installed on SCSE equipment.
- Only software used for legitimate SCSE business purposes may be installed.
- No software may be brought onto or taken from SCSE's premises without prior authorisation.
- Unauthorised access to SCSE systems, or unauthorised copying or removal of SCSE equipment or software, will result in disciplinary action under the Disciplinary and Grievance Policy and may lead to dismissal.

Virus protection

To prevent virus contamination of SCSE systems:

- Unauthorised software, including public-domain software, USBs, external hard drives, CDs or internet downloads, must not be used.
- All software must be virus-checked using SCSE's standard testing procedures before use.
- Any suspected malware or security incident must be reported to a Director immediately.

Internet use (staff)

The internet is available to staff for legitimate business use and matters directly concerned with the role. Where staff publish material in SCSE's name, content must be relevant to professional activities and must respect intellectual property and copyright. Where personal views are expressed online in any context that could be linked to SCSE, a clear disclaimer should be added that the views are personal.

SCSE will not tolerate use of the internet system for:

- Accessing websites that put SCSE's systems at risk (including via viruses) or that compromise SCSE's copyright or intellectual property rights.
- Conduct that breaches the Social Media Policy.

- Connecting to, posting, or downloading any information unrelated to your work, in particular pornographic, extremist, or otherwise offensive material.
- Computer hacking or related activities, or attempting to disable or compromise the security of SCSE systems.

The activities in the final two bullets above may also constitute a criminal offence.

Email use (staff)

The email system is available for SCSE business communications. Used appropriately, it supports efficiency; used inappropriately, it can cause confusion, harm, or legal exposure. The following applies:

- Comply with SCSE's communication standards, including the Code of Conduct.
- Send messages and copies only to those for whom they are relevant.
- Email should not be used as a substitute for face-to-face or telephone contact where the latter would be more appropriate, unless this is necessary as a reasonable adjustment for neurodivergence or disability — to be agreed with a Director on an individual basis.
- Do not send hasty or abusive emails. Messages sent without proper consideration can cause upset, concern or misunderstanding.
- Where an email contains confidential information, take the necessary steps to protect that confidentiality.
- Be aware that contracts and offers transmitted by email are as legally binding on SCSE as those sent on paper. Do not commit SCSE to anything by email without authorisation.

SCSE will not tolerate use of the email system for:

- Any messages that could constitute bullying, harassment, discrimination, or other detriment.
- Personal use beyond what is incidental (social invitations, jokes, chain letters and similar should not be sent through SCSE accounts).
- Online gambling.
- Accessing or transmitting pornography or other offensive material.
- Transmitting copyright information without authorisation.
- Posting confidential information about colleagues, learners, families, SCSE, or its partners.

Social networking sites (staff)

Staff use of social networking is governed by the Social Media Policy. In summary:

- Personal social media accounts must not present staff as official spokespeople for SCSE.
- Staff must not befriend or follow current learners on personal social media accounts.
- Posts that identify the poster as SCSE staff, or that refer to SCSE's work, learners, partners or funders, must comply with the Social Media Policy and the Safeguarding Policy.

Monitoring (staff)

SCSE reserves the right to monitor all email and internet activity for the purposes of ensuring compliance with SCSE's policies and procedures and with applicable regulatory requirements. This includes monitoring of any additional accounts staff are asked to set up for the purposes of their work, which are subject to the same rules as SCSE work accounts.

Information acquired through monitoring may be used as evidence in disciplinary proceedings. Monitoring involves processing of staff personal data; lawful basis, retention and access are covered in the employee privacy notice and the Secure Data Handling and Data Protection Policy.

10. Learner Acceptable Use Agreement (Under 18s)

The following plain-language version of this policy applies to every learner under the age of 18 attending SCSE. It is signed by the learner and (where the learner is under 16) by their parent or carer at induction. A copy is held in the learner's record.

What this agreement is for

It explains what you can and can't do online when you're using SCSE computers, tablets, Wi-Fi, or your own phone while you're with us. It also tells you what to do if anything online makes you feel unsafe, uncomfortable, or worried.

What we expect from you

- Use SCSE's computers, accounts and Wi-Fi for learning and the activities your tutor has set.
- Be kind and respectful in everything you write online – messages, chats, comments and posts. The way you treat people online matters just as much as the way you treat them in person.
- Keep your password to yourself. Don't log in as someone else, and don't let anyone else log in as you.
- If you see something online that worries you, frightens you, or doesn't feel right, tell a trusted SCSE adult straight away. You won't be in trouble for asking for help.
- Look after our equipment. Tell us straight away if something is broken, damaged or not working properly.
- If you bring your own phone, keep it on silent during sessions. We may ask you to put it away if it is getting in the way of your learning.

Things that are not OK

- Bullying, threatening, harassing or being cruel to anyone – in chat, in comments, in DMs, in games, or anywhere else.
- Sharing or asking for nudes, sexual images, or sexual messages. This is taken very seriously and may be a criminal offence.
- Looking at, downloading, or sharing pornography, extreme violence, or content that promotes hatred or terrorism.
- Trying to get into someone else's account, email, or files; trying to get around the school's filters or settings.
- Pretending to be someone else online to bully or trick them.
- Buying or selling things using SCSE accounts or equipment without permission.
- Recording, filming or photographing other learners or staff without their agreement, and sharing those recordings.

If something goes wrong online

Tell an SCSE adult you trust. You can speak to your mentor, the Designated Safeguarding Lead (Elizabeth Amos-Milburn) or the Deputy DSL (Alexandra Gager-Liebhart). If it's outside SCSE hours and it can't wait, you can also:

- Call 999 if you or someone else is in immediate danger.
- Call Childline on 0800 1111 (any time, free, in confidence).
- Use Report Remove (Childline / IWF) to remove a nude image of yourself from the internet.

What happens if you break this agreement

It depends on what's happened. We might have a conversation with you about it. We might restrict your access to certain systems for a while. We might involve your parent or carer or your commissioning school. If what's happened is a safeguarding concern or a possible criminal offence, we will follow our Safeguarding Policy, which may include involving the police or Children's Social Care.

Your signature

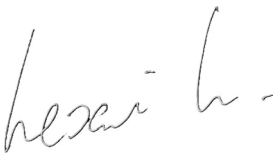
I have read this agreement (or had it read to me). I understand what is expected of me, what I should not do, and what to do if something goes wrong online.

Learner name	
Learner signature	
Date	
Parent / carer name (if learner under 16)	

Parent / carer signature	
Date	

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.