Online Safety and E-Safety Policy

Document Control

Document Title	Online Safety and E-Safety 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 how South Cumbria Skills Exchange (SCSE), operated by Whamos Training and Development CIC, keeps learners safe online while engaging with our provision, and how we educate learners to keep themselves safe more generally.

It is distinct from the Acceptable Use Policy. The Acceptable Use Policy sets out what users can and cannot do on SCSE systems. This Online Safety Policy sets out how SCSE actively safeguards learners from online harm.

This policy reflects KCSIE 2024 (especially Annex C on online safety), the Prevent duty, UK GDPR, and current UK Council for Internet Safety (UKCIS) guidance.

2. Scope

This policy applies to:

- All learners at SCSE, in any setting where they access digital tools as part of SCSE activity (CS Learner platform, filmmaking tools, online learning resources, communication tools)
- All staff, volunteers and contractors whose work involves the digital environment
- Any third-party platform used as part of SCSE delivery

It complements expectations in the Safeguarding Policy and reinforces the practical work undertaken in induction and ongoing learning.

3. The four key online safety risks (the “Four Cs”)

Following UKCIS, we recognise four categories of online safety risk:

- **Content** — exposure to age-inappropriate, harmful or illegal content, including pornography, violent content, extremist material, content promoting self-harm, eating disorders or suicide
- **Contact** — being approached or contacted by adults posing a risk (grooming, sextortion, recruitment to extremism, exploitation)
- **Conduct** — behaviour by the learner themselves or by peers that causes harm, including cyberbullying, sharing nudes (“sexting”), making threats, harassment, hate speech
- **Commerce** — financial harm including phishing, scams, gambling, online financial exploitation

Our approach addresses each of these.

4. Technical controls on SCSE systems

SCSE’s network and devices are configured to:

- Filter known categories of harmful content (pornography, violence, self-harm content, extremism, gambling, drugs, weapons)
- Monitor for keywords associated with safeguarding risk
- Log access activity for review where a concern arises
- Block installation of unauthorised software on SCSE devices
- Require strong passwords and screen locks
- Apply security updates within an agreed schedule

Filtering is not a substitute for adult supervision. Staff actively supervise learner use of digital tools rather than relying on filtering to catch every risk.

5. The CS Learner platform and other learning tools

Where SCSE uses an online learning platform (currently CS Learner) and other digital tools (filmmaking software, awarding-body portals, communication tools), the following applies:

- Each learner has their own credentials, never shared
- Learners' activity on the platform is visible to their tutor and the Directors
- Communication via the platform is monitored
- Personal data on the platform is processed under our Secure Data Handling and Data Protection Policy
- Vendor assurance (terms of use, data processing agreement, security posture) is reviewed before adoption and annually thereafter

6. Personal devices on site

Learners' personal devices on site are governed by the Acceptable Use Policy. In summary, devices may be permitted with the agreement of the session lead but are not to be used to:

- Photograph or record staff or peers without consent
- Access content that breaches the Acceptable Use Policy
- Communicate with people outside the session in a way that disrupts learning
- Bypass SCSE network filtering (e.g. via mobile data) to access restricted content

Where a learner's personal device use is causing concern, the session lead can ask the learner to put the device away. Devices are not confiscated; if a learner does not comply, the session lead consults the Director.

7. Online safety in the curriculum

SCSE builds online safety into induction and throughout the learning experience. Topics covered include:

- Privacy and personal information (what to share, what not to share, with whom)
- Recognising grooming and online manipulation
- Cyberbullying: recognising, responding, reporting
- Sharing of nudes, "sexting", and the law
- Online consent and respectful behaviour
- Critical evaluation of content (fake news, manipulated images, AI-generated content)
- Online radicalisation and extremism (in line with the Prevent Policy)
- Healthy use of social media, including managing screen time and the impact on mental health
- Online gambling and financial scams
- Online gaming safety
- The role of moderation, reporting and blocking

The curriculum is adjusted to the age and developmental stage of each learner, and to specific risks identified in their support plan.

8. Online safety in filmmaking work

Filmmaking work raises distinctive online safety considerations:

- Sharing draft material between team members via secure channels
- Protecting against unauthorised use or re-distribution of footage
- Managing the digital footprint of subjects who appear on camera
- Considering the impact of public-facing online distribution on the long-term digital presence of the learner

These are addressed both technically (secure platforms, watermarking where appropriate, deletion of working files after project completion) and educationally (briefing learners on the long tail of online content).

9. Reporting online safety concerns

A learner who has an online safety concern can:

- Speak to any member of SCSE staff
- Speak specifically to the Designated Safeguarding Lead (Elizabeth Amos-Milburn) or Deputy DSL (Alexandra Gager-Liebhart)
- Use the anonymous reporting box at reception
- Use the in-platform reporting tool where available

External reporting routes (also displayed in the learning space):

- **CEOP (Child Exploitation and Online Protection)** — ceop.police.uk — for concerns about online sexual abuse or contact
- **Internet Watch Foundation** — iwf.org.uk — for reporting child sexual abuse images
- **Report Harmful Content** — reportharmfulcontent.com — for reporting content that breaches platform standards
- **Revenge Porn Helpline** — 0345 6000 459 — for support with non-consensual intimate image sharing
- **Childline** — 0800 1111 — free, confidential support
- **Police** — 999 in emergency, 101 for non-emergency

10. Responding to an online safety concern

When SCSE becomes aware of an online safety concern, the DSL coordinates the response. Specific scenarios:

Online sexual abuse, grooming, or exploitation: Follow the Safeguarding Policy. Refer to police (CEOP) and to Children's Social Care. Preserve evidence (do not delete messages, keep screenshots). Do not view or copy any image of child sexual abuse — this is a criminal offence.

Sharing of nudes between learners ("sexting"): Follow UKCIS Sharing Nudes and Semi-Nudes guidance. Do not view, copy or forward the image. Refer to the DSL, who will assess and may refer to police and Children's Social Care.

Sextortion (threats to share intimate images): Treat as a serious safeguarding matter. Reassure the learner. Preserve evidence. Refer to police. Do not pay any demand. Report to Report Remove (NSPCC and IWF service for under-18s).

Online radicalisation: Follow the Prevent Policy. Notify the Prevent Lead the same day.

Cyberbullying: Follow the Anti-Bullying Policy.

Self-harm or suicide-related content: Follow the Mental Health Policy and Safeguarding Policy. Where there is immediate risk to life, call 999. Notify parent/carer and commissioning school.

Inappropriate adult contact (not necessarily sexual — e.g. coercion, financial scam): Treat as a safeguarding concern and refer to the DSL.

11. Working with parents and carers

SCSE supports parents and carers in their own role keeping children safe online:

- Information signposted at induction (NSPCC, Internet Matters, UK Safer Internet Centre)
- Where a learner's home internet use is causing concern, we work with the parent or carer and where appropriate the commissioning school to agree a coordinated approach
- We do not assume parents have the same level of digital literacy as their child; conversations are pitched accordingly

12. Working with commissioning bodies

For learners placed with SCSE, online safety concerns are shared with the commissioning school's DSL in the same way as any other safeguarding matter. Information is shared promptly, proportionately, and with consent where consent is required.

13. Staff online safety training

All staff complete:

- Annual safeguarding training that includes online safety
- Specific training in response to new threats or platforms
- Prevent training (including online radicalisation)
- Briefing on safer practice in any specific tool SCSE adopts

The DSL and Deputy DSL complete additional online safety training including how to respond to nude-sharing incidents and sextortion.

14. Online safety incident log

All online safety incidents are recorded in the safeguarding log. The Directors review the log monthly to identify trends and inform any policy or curriculum update.

15. Working with awarding bodies and external platforms

Where SCSE delivers awarding-body content via online tools, we ensure the platform meets appropriate data protection and safeguarding standards before adoption. Where a platform's standards prove inadequate during use, SCSE will raise concerns with the vendor and, if necessary, withdraw from use.

16. AI and generative tools

Where learners use generative AI tools (e.g. for drafting, ideation, image generation as part of a creative project), the Plagiarism Policy applies. From an online safety perspective, learners are taught to:

- Be cautious about personal information shared with AI tools
- Critically evaluate AI output
- Understand that AI-generated content may itself be harmful or misleading
- Recognise the implications of using AI to generate images of people, including consent

17. Confidentiality

Online safety concerns are handled in line with the Confidentiality Policy and the Secure Data Handling and Data Protection Policy. We do not promise confidentiality to a learner who raises a concern; we explain who we may need to tell and why.

18. Related policies

This policy should be read alongside:

- Safeguarding Policy
- Acceptable Use Policy
- Anti-Bullying Policy
- Social Media Policy

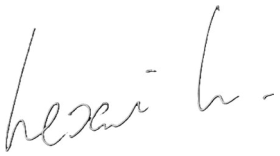
- Prevent and Anti-Radicalisation Policy
- Mental Health Policy
- Photography, Filming and Image Use Policy
- Plagiarism Policy
- Secure Data Handling and Data Protection Policy
- Terms of Use, Remote Access and User Monitoring Policy

19. Policy review

This policy is reviewed annually by the DSL and Directors, or sooner if statutory guidance, the online safety landscape, or our digital tools change.

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.