

Online and Digital Safety Policy

Field	Description
Document title	Online and Digital Safety Policy
Version	V5.0
Author	DSL
Date issued	10/09/2026
Status	Approved
Approved by	Trustees
Review date	10/09/2027
Document location	Document Control SharePoint - Safeguarding

1. Introduction

Step Into Learning recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology to enhance skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

This policy is written in line with statutory safeguarding guidance including *Keeping Children Safe in Education (KCSIE) 2026* (effective 1 September 2026), and reflects Ofsted expectations for safeguarding to be effective, proactive and embedded across the organisation. It also aligns with the Online Safety Act 2023, DfE Digital and Technology Standards, and the four categories of online harm (the 4Cs): Content, Contact, Conduct, Commerce.

Our approach is to implement safeguards to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance, and the implementation of our associated policies.



We recognise that safeguarding incidents can occur both online and offline, and that online safety is a key component of our safeguarding culture. Online safety protections apply equally whether learners are on-site, off-site, or accessing systems remotely.

Trustees receive annual assurance on the effectiveness of online safety arrangements.

2. Scope

This policy applies to all staff, trustees, learners, parents, contractors, volunteers, agency/supply staff and visitors to Step Into Learning. It covers all internet-connected and electronic devices — organisation-owned and personal — when accessing organisation systems or communicating with learners, on-site or off-site.

3. Definitions

- Approved systems: Organisation-provided and managed platforms, email, messaging and learning environments only.
- Making or sharing nudes and semi-nudes: Creating, sending, receiving or distributing intimate images — including photographs, video, livestream, and AI-generated/deepfake imagery — regardless of apparent consent; always a safeguarding concern.
- The 4Cs: Framework for assessing online risk — Content (harmful material), Contact (grooming/exploitation), Conduct (bullying, coercion, abuse), Commerce (scams, trafficking, financial exploitation).
- DPIA: Data Protection Impact Assessment — mandatory before deploying new monitoring, filtering or AI tools.
- DSPT: Data Security and Protection Toolkit — a framework used for assurance purposes; not a statutory requirement for this organisation. Used as good-practice reference only.

4. Policy Statement

4.1 Monitoring Usage

Step Into Learning actively monitor learners and staff use of IT systems and IT network usage as part of their responsibility towards safeguarding.

Monitoring is conducted proportionately and lawfully to identify risks, including abuse, exploitation, radicalisation, bullying, harmful sexual behaviour,



child-on-child abuse, and making or sharing nudes and semi-nudes (including AI-generated imagery).

Users are made aware that monitoring takes place, and that activity may be recorded for safeguarding, security and compliance purposes. A published privacy notice explains: what is monitored, lawful basis, who may view data, retention periods, and rights of appeal. A full Data Protection Impact Assessment (DPIA) — documenting necessity, proportionality, risk assessment, safeguards, and ICO consultation where required — is completed and approved before deploying or changing any monitoring, filtering, or AI system.

Where there are any concerns, these are logged and reported immediately to the Designated Safeguarding Lead (DSL).

Filtering and monitoring systems:

- Reviewed at least annually by a named Senior Leadership Team member, supported by DSL and IT support; trustees receive a summary report.
- Reviewed out-of-cycle whenever new risks emerge or new tools (including generative AI) are introduced.
- Designed to meet or exceed DfE Filtering and Monitoring Standards.

4.2 Cybersecurity

Step Into Learning's IT systems and Information Security Management System are certified to Cyber Essentials Information Security and Cyber Security standards.

These standards are regularly reviewed by independent experts providing staff, learners & stakeholders reassurance that Step into Learning IT systems cybersecurity follow the highest levels of best practice.

Step Into Learning fully aligns with the National Cyber Security Centre (NCSC) guidance and the Cyber Essentials Scheme.

Staff and learners must:

- Use strong passwords and not share credentials
- Report phishing, suspicious emails, or security concerns immediately
- Not install unauthorised software or connect unapproved devices
- Use only approved AI tools — any AI tool used with learner data must have a Data Protection Impact Assessment (DPIA) and safeguarding risk assessment completed and approved in advance

Any breach of the Computer Misuse Act 1990 including all forms of hacking or acquiring/accessing someone else's digital identity is a criminal offence and will be referred appropriately.

All cybersecurity incidents are reported to the DSL without delay; major breaches are reported to trustees and relevant authorities within 24 hours.

4.3 Communication Between Staff and Learners

Staff must ensure that:

- Safe and responsible online behaviours are modelled and promoted
- Communication occurs within clear, explicit professional boundaries
- All communication is transparent, auditable, and open to scrutiny
- Only approved organisational systems are used; communication occurs during reasonable working hours (typically 08:00–17:00 term-time) and relates solely to educational/work-placement matters
- Out-of-hours or holiday communication is permitted only in pre-agreed, supervised circumstances
- No personal conversations, inappropriate language, sharing of personal contact details, or boundary-blurring communication
- Staff must not share personal information with any learner
- Staff must not accept or initiate contact with learners via personal social media — this is a safeguarding rule, not guidance
- One-to-one online meetings must be pre-approved, scheduled, and observable or recorded

All communication must:

- Take place via approved organisational systems only
- Be professional, transparent, and auditable
- Never occur via personal devices or private accounts

Staff must not:

- Engage in private or one-to-one messaging outside approved systems
- Create or accept personal social media connections with any learner

4.4 Social Networks and Online Risks

Step Into Learning uses social media channels to share information and engage appropriately. We recognise that evolving risks include:

- Content: extremist/pornographic/harmful material, misinformation/disinformation/conspiracy theories, AI-generated abusive content
- Contact: grooming, exploitation, harmful connections



- Conduct: cyberbullying, harassment, coercion, making or sharing nudes/semi-nudes, child-on-child abuse
- Commerce: scams, trafficking, financial exploitation

Learners are taught how to identify, report and seek help for all the above risks as part of a planned curriculum. All incidents involving intimate imagery — including AI-generated/deepfakes — are referred to the DSL and treated as safeguarding concerns, regardless of whether the images were described as “consensual”.

4.5 Use of Images and Video

Images and video support learning but carry specific safeguarding risks including AI scraping and deepfake abuse. Before publishing any image of a learner:

- Explicit, informed consent is obtained — consent forms must specifically warn that images may be scraped and used to create abusive imagery
- Under-18 learners must not be named alongside their image
- Group photographs are preferred; avoid identifiable individual portraits where possible
- Images are assessed for safeguarding risk before publication
- A publication expiry/removal date is recorded
- Images are stored securely and accessed only by authorised staff
- Copyright and intellectual property rights are respected at all times

4.6 Personal Data and Data Protection

Personal data is processed lawfully, fairly and transparently in line with the Data Protection Act 2018 and UK GDPR.

We apply:

- Lawful basis for all processing
- Data minimisation and purpose limitation
- Role-based access and secure storage
- Defined retention and deletion schedules
- Staff must:
 - Only access data necessary for their role
 - Report any data breach immediately to the DSL; breaches involving learner data are escalated to the ICO and safeguarding authorities without delay
 - Comply fully with the separate Data Protection Policy

4.7 Security

Technical safeguards include enterprise-grade filtering, firewalls, secure network configuration, endpoint protection, and regular vulnerability testing to prevent

unauthorised access. Security measures are reviewed annually and whenever new risks emerge.

4.8 Online Safety and Mobile Devices

Step Into Learning adopts a whole-organisation approach to online safety in line with KCSIE and Ofsted expectations.

Key measures include:

- Effective filtering and monitoring systems (DfE standards) reviewed annually
- Regular risk reviews covering all 4Cs and emerging threats including generative AI
- Age-appropriate online safety education for all learners
- Clear reporting mechanisms for concerns

Online risks include (but are not limited to):

- Sexual exploitation and abuse
- Radicalisation
- Cyberbullying
- Exposure to harmful content
- Online harassment
- Fraud and scams
- Misinformation
- Disinformation
- Conspiracy theories
- AI-generated content

5. Implementation

5.1. Role and Responsibilities

All staff must:

- Read KCSIE Part One in full annually — recorded on the Single Central Record
- Understand that safeguarding incidents occur online or offline; report all concerns immediately; recognise indicators of abuse; maintain vigilance
- Promote safe practice; model positive digital behaviour
- Communicate professionally and in line with this policy at all times
- Protect personal data; work only on secure devices; log off after sessions
- Report concerns about other staff's behaviour through safeguarding procedures

Learners must:

Follow the IT Acceptable Use Code of Conduct

- Report any online concern involving themselves or others to a trusted member of staff
- Use technology responsibly and respectfully
- DSL / DDSL must:
- Identify, record and respond appropriately to all online safety concerns
- Oversee filtering/monitoring; ensure annual review; report termly to Leadership Team and annually to Trustees
- Maintain robust DSL cover arrangements at all times
- Refer extremist-content incidents to Prevent where appropriate
- Ensure all online safety training and awareness is up-to-date

IT Support must:

- Maintain secure infrastructure meeting best practice
- Record, investigate and resolve security incidents promptly
- Report concerns to the DSL immediately

Trustees must:

- Receive annual assurance on online safety effectiveness
- Oversee policy compliance and approve major changes

5.2. Training and Guidance

Mandatory training for all staff includes:

- KCSIE Part One (read and confirmed annually)
- Online safety risks, trends and the 4Cs framework
- Recognising abuse, exploitation, harassment and making/sharing nudes
- AI risks and safe, responsible use
- Filtering and monitoring awareness
- Data protection responsibilities
- Mobile phone policy and enforcement
- Radicalisation, extremism and Prevent awareness

DSL/DDSL: receive enhanced, up-to-date training including KCSIE changes, AI risks and online harms.

Learners: receive ongoing age-appropriate education covering safe practice, risk recognition, healthy relationships, AI/deepfake awareness, and how to seek help.

5.3 Publishing Material Online

Before publishing any content including images:

- Consent is obtained and fully informed (including AI-related risks)



- No under-18 is named alongside their image
- Group photos preferred; individual portraits avoided where possible
- Safeguarding risk assessment completed
- Copyright respected
- Expiry/removal date set

6. Legislation and Guidance

- Keeping Children Safe in Education (KCSIE) 2026
- Online Safety Act 2023
- Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025) / UK GDPR
- Computer Misuse Act 1990
- Counter-Terrorism and Security Act 2015 (Prevent duty)
- Human Rights Act 1998
- DfE Digital and Technology Standards (including Filtering & Monitoring)
- RSHE Statutory Guidance
- Mobile Phones in Schools – Statutory Guidance (DfE)
- NCSC / Cyber Essentials Scheme