

Achievement Training & Skills

Online Safety Policy

2026–2027

Document Revision

Issue Date	01 Jul 2019	Authorised by: E. Johnson (Chief Operations Officer)
Review Date	01 Sep 2026	Signature: E. Johnson (Chief Operations Officer)
Next Review Date	01 Sep 2027	Appointment: E. Johnson (Chief Operations Officer)
All company policies are to be reviewed by the Chief Operations Officer annually or earlier where circumstances dictate.		

Achievement Training & Skills (ATS) Online Safety Policy

This policy has been updated to align with Keeping Children Safe In Education (KCSIE) 2026 and reflects current safeguarding expectations relating to online safety, including Artificial Intelligence (AI), filtering and monitoring, online abuse and digital safeguarding.

Introduction

ATS recognises that online safety is an essential element of safeguarding and promoting the welfare of children, young people and vulnerable adults. Technology offers significant educational benefits but also presents evolving risks. ATS is committed to creating a culture where learners and staff use technology safely, responsibly and respectfully through education, robust procedures, effective filtering and monitoring, and timely reporting of concerns. ATS recognises the benefits and opportunities that new technologies offer to teaching and learning. Our approach is to implement safeguards within the organisation and support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training, guidance and the implementation of associated policies. In furtherance of our duty to safeguard learners, we will do all that we can to help our learners and staff stay safe online and to satisfy our wider duty of care. This Online Safety Policy should be read in conjunction with other relevant company policies and procedures, such as Safeguarding, Sexual Harassment and Anti-Bullying Policies, and company Disciplinary policies.

Definition of Online Safety

For the purposes of this policy, online safety refers to the safeguarding of children, young people, vulnerable adults and staff when using digital technologies, the internet and connected devices. It encompasses the safe, responsible and respectful use of technology, both within and outside of the learning environment.

ATS recognises that online safety is a fundamental part of safeguarding and child protection. Online risks continue to evolve rapidly and can affect learners both during and beyond their learning programme. Effective online safety requires a whole-organisation approach, combining appropriate policies and procedures, staff training, learner education, filtering and monitoring systems, and a culture where concerns are recognised and reported promptly.

Online safety risks can be grouped into four broad categories:

1. Content

Learners may be exposed to harmful, illegal or inappropriate online material, including:

- Age-inappropriate content.
- Extremist or terrorist material.
- Misinformation and disinformation.
- Violent, hateful or discriminatory content.
- Self-harm, suicide or eating disorder content.
- Sexually explicit material.
- AI-generated or manipulated content (including deepfakes).

2. Contact

Learners may be subjected to harmful interactions with others online, including:

- Grooming and child sexual exploitation.
- Radicalisation.
- Online coercion or manipulation.
- Sextortion.
- Bullying, harassment or stalking.
- Contact from individuals seeking to exploit or financially abuse others.

3. Conduct

Learners may behave in ways online that place themselves or others at risk, including:

- Cyberbullying.
- Sharing indecent images.
- Online abuse or hate speech.
- Creating or sharing harmful AI-generated content.
- Inappropriate use of social media or messaging platforms.
- Breaches of privacy or confidentiality.

4. Commerce

Learners may be exposed to financial risks online, including:

- Online scams and fraud.
- Phishing attempts.
- Identity theft.
- Gambling.
- Unsafe online purchasing or financial exploitation.

Scope

The policy applies to all persons who have access to company IT systems, both on premises and through remote access. Any user of company IT systems must adhere to online safety rules. The Online Safety Policy applies to all use of the internet and electronic communication devices, such as email, mobile phones, games consoles, social networking sites and any other systems that use the internet for connection and providing information.

Aims

- Promote a strong culture of online safety.
- Protect learners and staff from online harm.
- Ensure legal compliance, including UK GDPR and the Data Protection Act 2018.
- Provide appropriate education, filtering, monitoring and reporting arrangements.
- Respond promptly and effectively to online safety concerns.
- To ensure safeguards on company IT-based systems are strong and reliable.
- To assure that the storage and use of images and personal information on company-based systems is secure and meets all legal requirements.
- To educate staff and learners in online safety.
- To ensure any incidents which threaten online safety are managed appropriately.

Emerging Online Risks

ATS recognises risks including AI misuse, deepfakes, misinformation, cyberbullying, sextortion, online grooming, radicalisation, phishing, scams, identity theft, harmful online communities, image-based abuse and online sexual harassment.

Filtering and Monitoring

ATS will ensure proportionate filtering and monitoring arrangements are in place to help identify safeguarding concerns while supporting legitimate teaching and learning. Any concerns identified will be reviewed promptly and escalated to the Designated Safeguarding Lead (DSL) where appropriate.

Use of Images and Video

The use of images, photographs and video is encouraged where appropriate to support teaching and learning, provided that copyright, intellectual property rights, privacy and other legal rights are respected.

Staff and learners will receive appropriate guidance on the risks associated with downloading, creating, posting and sharing images and video. This includes awareness of the potential risks of sharing personal images or videos on social media and other online platforms.

Learners will be provided with information and guidance on the appropriate and responsible use of images and videos, including how to protect their personal information, privacy and digital identity.

Staff and learners must gain permission and consent before taking, using, publishing or sharing images or videos of others.

Staff must ensure that any images or videos used within teaching, learning or organisational materials are appropriate, relevant and do not compromise the dignity, privacy or safety of staff, learners or any other individual.

Staff Responsibilities

Staff are expected to model safe, responsible and professional online behaviour at all times and to recognise that their conduct online can have an impact on learners, colleagues, employers and the reputation of ATS. Staff must maintain appropriate professional boundaries when using digital technology and communicating with learners, including through email, messaging platforms, social media, video conferencing and other online channels.

Staff must:

- Model appropriate online behaviour by communicating professionally, respectfully and appropriately across all digital platforms and demonstrating the standards expected of learners.
- Maintain professional boundaries with learners and colleagues when using technology and social media. Staff should not engage in inappropriate online relationships, communications or interactions with learners and must follow ATS guidance regarding contact with learners outside approved systems.
- Complete regular safeguarding and online safety training and ensure that they remain familiar with current ATS policies, procedures and expectations relating to online safety, safeguarding, data protection and acceptable use of technology.
- Report safeguarding and online safety concerns immediately through the appropriate ATS reporting procedures. This includes concerns relating to inappropriate online behaviour, exploitation, grooming, cyberbullying, harassment, harmful or illegal content, or any activity that may place a learner or another individual at risk.
- Use AI responsibly and ethically, ensuring that AI tools are used in accordance with ATS policies and applicable data protection and confidentiality requirements. Staff must not enter confidential, personal or sensitive information into AI systems unless this has been specifically authorised and is appropriate to do so.
- Protect confidential and personal information and comply with UK data protection requirements and ATS policies. Staff must take appropriate steps to prevent unauthorised access, disclosure, loss or sharing of learner, staff, employer or organisational information.

- Use ATS systems, devices, accounts and digital resources appropriately, only for legitimate purposes and in accordance with relevant policies and procedures.
- Consider the potential impact of online activity before posting or sharing content. Staff should be aware that content posted online may be permanent, can be copied or shared by others, and may be associated with them professionally even when posted through a personal account.
- Ensure that personal views expressed online cannot reasonably be interpreted as representing the views of ATS, particularly where staff identify themselves as working for, or are otherwise visibly associated with, the organisation.

Learner Responsibilities

Learners are expected to use technology responsibly, safely and respectfully at all times, both during their training and when representing ATS online. This includes using devices, systems, platforms, social media and online communication appropriately and in accordance with ATS policies and procedures.

Learners should:

- Use technology responsibly and only for appropriate, lawful and legitimate purposes.
- Treat others with respect online, including staff, fellow learners, employers, and members of the wider community. Online behaviour should reflect the same standards of professionalism and respect expected in face-to-face interactions.
- Report any concerns relating to online safety, cyberbullying, harassment, inappropriate or harmful content, suspicious activity, or anything that makes them feel unsafe or uncomfortable to the DSL.
- Avoid creating, accessing, sharing or storing inappropriate, offensive, discriminatory or harmful content, including images, videos, messages or other material that could negatively affect themselves or others.
- Protect personal and confidential information by keeping passwords secure, using appropriate privacy settings and taking care when sharing information, photographs or other content online.
- Respect the privacy of others and do not share another person's personal information, images, recordings or content without their knowledge and consent.
- Follow ATS' policies and procedures.
- Use ATS systems and resources appropriately.

Learners may use AI tools responsibly to support their learning, where this is permitted by ATS and the requirements of their apprenticeship or programme. AI can be a useful learning tool, but it should support rather than replace the learner's own knowledge, skills, judgement and work.

Personal Information

Personal data will be processed in accordance with UK GDPR and the Data Protection Act 2018. Confidential information is stored securely and is only accessible by authorised individuals. Staff must always keep learner's personal information safe and secure.

Education and Training

Online safety education will be embedded throughout the learner journey and through staff Continuous Professional Development (CPD). Topics include healthy relationships, consent, digital footprints, privacy settings, misinformation, scams, AI, cyberbullying and reporting concerns.

Incident Reporting

All online safety concerns must be reported immediately to the DSL and managed in line with the Safeguarding Policy. Serious incidents may be referred to external agencies where appropriate.

Monitoring and Review

This policy will be reviewed annually, or sooner where legislation, statutory guidance or organisational needs require.