Policy Name	E-Safety Policy
Policy Lead	Safeguarding Team
Original Issue Date	July 2024
Last Review Date	November 2025
Next Review Date	November 2026
Version	3
Authorised by	SMT
Signature/Board Ref	Approved

Contents of this policy document

Revision History

Version	Type	Date	Notes
1	New	July 2024	New issue
2	Reviewed	November 2024	Addition of further context to the Smoothwall Monitoring system on page 8 & 11.
3	Amendment	November 2025	Addition of AI related risks into Policy and Annex A (AUP)
4			
5			

1. Rationale

The purpose of the e-Safety policy at WS Training Ltd is to safeguard and promote the welfare of all members of our community when using technologies both on-site and at home. Online safety is a critical component of our safeguarding efforts, and we are committed to ensuring that all learners and staff are protected from potential harm when using mobile technology or social media. Mobile devices, such as computers, tablets, mobile phones, smartwatches, and game consoles, along with social media, play an integral role in daily life, offering both opportunities and challenges. WS Training Ltd aims to empower our learners to acquire the knowledge needed to use mobile technology and social media safely, respectfully, and responsibly. We strive to develop high levels of digital skills and resilience in our learners to manage and respond to online risks, preparing them for future learning opportunities and employment.

This policy considers the DfE statutory guidance 'Keeping Children Safe in Education' 2024 and the PREVENT Duty, as well as DfE Guidance 'Sharing nudes and semi-nudes – advice for education settings working with children and young people' (2020). It also acknowledges that learners may undertake at least 25% of their learning remotely and might increase this proportion in response to a full or partial closure. In the event of a transition to full-time remote learning, WS Training Ltd will adhere to statutory guidance, recognizing the lessons learned during the pandemic.

This policy also incorporates the UKCIS digital resilience framework, 2020, which provides a structure for building resilience in the digital lives of staff and learners. The framework's four components—Understand, Know, Learn, and Recover—are explored through the e-safety component of our Professional Development curriculum.

2. Aims

This policy applies to all users, including learners, staff, and all members of the WS Training Ltd community who have access to our IT systems, both on the premises and remotely, and to those using their personal devices on the premises. The E-Safety Policy covers all use of the internet and electronic communication devices such as email, mobile phones, game consoles, and social networking sites and apps.

While this policy primarily refers to the use of technology for company-related teaching and learning activities—whether on our premises via the WS Training Ltd Wi-Fi network or remotely—it also applies to incidents such as cyberbullying, sexual harassment online, and the consensual and non-consensual sharing of nude and semi-nude images and videos. This includes revenge porn and technology-assisted harmful sexual behaviour, which may occur outside of provision but impact our community, individuals, or reputation.

3. Risks

There are numerous risks and dangers associated with young people's use of technology, which can impact their safety or security. The policy categorises these risks as follows, based on Annex C of Keeping Children Safe in Education 2024:

- **Content:** Access to illegal, harmful, or inappropriate images or other content.
- **Contact:** The risk of grooming by individuals contacted online.
- **Conduct:** Unauthorised access to or sharing of personal information.
- **Commerce:** Commerce is about the risk from things

Some of the dangers that may be faced:

Content	Contact	Conduct	Commerce
Access to illegal, harmful or inappropriate images or other content e.g. harmful challenges and on-line hoaxes	The risk of being subject to grooming by those with whom they make contact on the internet;	Unauthorised access to / loss of / sharing of personal information	
Access to unsuitable video / internet games/gambling sites	Inappropriate communication / contact with others, including strangers, for example through social networking sites	Making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and or pornography)	Online - Gambling
An inability to evaluate the quality, accuracy and relevance of information on the internet		Cyber-bullying	Inappropriate advertising
Plagiarism and copyright infringement		Race Hatred	Phishing and/or financial scams If you feel your learners or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).
		Terrorism extremism	
		Financial Abuse	
		Illegal downloading of music or video files	
The potential for use which may impact on the on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - Access or exposure to illegal / inappropriate materials	The potential for use which may impact on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - inappropriate on-line contact with adults / strangers - potential or actual incidents of grooming - cyber-bullying	The potential for use which may impact on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: - cyberbullying - Inappropriate portrayal of self to others.	

While it is impossible to eliminate these risks entirely, it is essential to build learners' resilience, providing them with the confidence and skills to manage and respond to these risks. This resilience is developed through our professional development curriculum throughout the year.

4. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities for individuals and groups within the organisation.
The company acknowledges that many learners have unrestricted internet access through mobile phone networks. Consequently, some learners may use their mobile or smart technology to engage in behaviours such as:

- Sexually harassing peers while on campus
- Sharing consensual or non-consensual nude images, often through large social media chat groups
- Accessing and distributing pornography and other harmful content, including revenge porn

In cases where such incidents are reported to staff, they are required to notify MyConcern. This allows for appropriate actions and support to be determined.

Safeguarding and Prevent Team
This group has strategic oversight of matters related to e-safety, reporting through the Safeguarding and Prevent Operational Team.

The group, comprising various representatives, and developers, is responsible for:

- Establishing and reviewing e-safety policies.
- Advising on e-safety guidelines for staff and learners.
- Planning e-safety activities, including inductions, professional development sessions, and safer internet day.
- Reviewing the impacts of new technologies, including Artificial Intelligence (AI), and monitoring trends in e-safety incidents.

Senior Management Team
The senior management team is responsible for ensuring the safety (including e-safety) of WS Training Ltd community members and will take appropriate actions in line with relevant policies. This includes ensuring policies reflect emerging risks associated with AI, including deepfakes, AI-generated misinformation, and potential breaches of privacy.

IT Services
IT Services is responsible for ensuring the security of WS Training's IT infrastructure, meeting e-safety technical requirements, enforcing password protection policies, and updating internet and anti-spam filtering policies regularly. Additionally, IT Services implements safeguards to prevent unauthorised AI-driven data collection, content generation, and misuse within company systems. They also regularly review AI-based security threats, such as phishing scams and AI-generated cyber-attacks.

Teaching and Support Staff

Teaching and support staff must ensure they:

- Read and understand the company's E-safety and Acceptable Use policy.
- Ensure learners are aware of e-safety and follow the company's E-Safety Policy, IT Acceptable Use Policy, and the Learner and Apprentice Code of Conduct.
- Safely use specified technologies as part of teaching and learning.
- Complete CPD/training as required by the company.
- Stay updated on e-safety matters.

- Being aware of AI-generated content risks, such as deepfakes, AI-assisted cheating, and misinformation.
- Report any suspected misuse or issues, including cyberbullying, sexual harassment, or sharing of nudes and revenge porn. Report incidents via MyConcern to ensure appropriate actions and support are identified. Follow-up will consider advice from relevant government publications.
- Monitor IT activity in lessons, whether on site or remotely, including learner use of company-related e-learning facilities, extracurricular, and extended site activities.
- Educating learners on the responsible use of AI, including ethical considerations and data privacy concerns.
- Engage with learners on social media within the guidelines of the IT Acceptable Use Policy, using only organisation accounts to safeguard both parties and manage expectations.

Learners

Learners are expected to:

- Be aware of the company's commitment to addressing peer-on-peer abuse, including sexual harassment online.
- Use company IT systems, communication tools, and mobile devices in accordance with the IT Acceptable Use Policy, which they agree to during induction and each time they access the Company IT system.
- Adhere to the Learner and Apprentice Code of Conduct for e-Learning found in the learner handbooks.
- Seek assistance and discuss concerns regarding e-safety incidents involving themselves or others within the setting.
- Understand the importance of reporting abuse, misuse, or exposure to inappropriate content, and know the appropriate reporting channels – either within the educational provision or directly to social media platforms.
- Understanding the potential risks associated with AI, such as deepfakes, misinformation, and biased content generation.
- Using AI tools responsibly in learning and research while adhering to academic integrity policies.
- Familiarise themselves with the policies regarding the use of mobile phones, digital cameras, and mobile devices, as well as policies on image-taking/use and cyberbullying.
- Recognise the significance of adopting responsible e-safety practices when using digital technologies outside of provision and acknowledge that the IT Acceptable Use Agreement applies to their actions related to all e-safety practices.

Apprentice

It is essential that all apprentices understand their responsibilities in the workplace and during any training with WS training. The responsibilities include:

- Follow the E-Safety policies set by your employer and WS Training. This includes using the internet, digital communication tools, and other IT resources responsibly and safely.
- Be aware of the potential risks associated with online activities, including cyberbullying, exposure to inappropriate content, and data breaches. Ensure that your actions online do not compromise your safety or that of others.
- If you encounter any E-Safety issues, such as cyberbullying, inappropriate content, or any activity that makes you uncomfortable, report it immediately to your employer or WS Training. It is important to speak up if something doesn't feel right.
- When using social media or other online platforms, maintain a professional demeanour that reflects positively on both your employer and WS Training. Avoid engaging in any behaviour online that could be harmful or inappropriate.

- Protect your personal information and that of your employer by following best practices for data security. This includes not sharing sensitive information online and using secure passwords.

Employers
Employers of apprentices have a crucial role in ensuring that their apprentices stay safe online and adhere to E-Safety laws. The responsibilities are:

- Ensure that your apprentice/s are aware of and understand your company's IT and E-Safety policies, including the responsible use of the internet and digital communication tools within the workplace.
- Ensuring apprentices understand workplace AI policies, particularly regarding data privacy, misinformation, and ethical AI use.
- Implement appropriate monitoring systems to oversee the online activity of apprentices, ensuring that they are following company guidelines and staying safe online. This includes being aware of any potential risks related to cyberbullying, inappropriate content, or breaches of data security.
- Facilitate ongoing education and training on E-Safety for your apprentices, keeping them informed of best practices and legal obligations regarding online behaviour and data protection.
- Actively enforce E-Safety policies and take appropriate action if an apprentice is found to be violating E-Safety rules. This includes collaborating with WS Training to ensure consistency in E-Safety expectations between the workplace and the Company.
- Make available the necessary resources and support for apprentices to report any E-Safety concerns or issues they encounter in the workplace, ensuring they feel confident in speaking up and seeking help

5. Acceptable Use

WS Training Ltd has IT Acceptable Use Policies to inform all their responsibilities, acceptable and unacceptable use, and consequences of misuse. The organisation will not tolerate any abuse of IT systems and will handle incidents of bullying, harassment, or other unacceptable conduct in line with the Behaviour policy and code of conducts. Illegal conduct will be reported to the police.

6. Communications

Computers, tablets, mobile phones, smart watches, games consoles, apps, social media, and other smart technologies offer various avenues for online communication, alongside challenges and potential risks. All digital interactions with learners must consistently uphold a professional tone and content, aligning with the staff code of conduct.

Staff responsibilities include:

- Avoiding the sharing of personal email accounts or home/mobile telephone numbers with learners.
- Refraining from adding learners as friends on personal social networking sites, and vice versa.
- Ensuring that any private social networking sites or blogs they participate in are clearly distinguished from their professional role.
- Using company-provided devices or learners' own devices for capturing images of the learners, or staff, rather than personal digital cameras or camera phones.
- Abstaining from any online activities that could compromise their professional duties.
- Following guidelines for social media use as outlined in the Acceptable Use Policy and Remote Working.

Learner obligations include:

- Not requesting staff members as friends on personal social networking sites, nor adding them as friends on such platforms.
- Adhering to the company's guidelines for remote and online learning.
- Refraining from engaging in online communications that involve bullying or harassment.
- Promptly reporting any incidents of which they are aware or have experienced to a staff member for swift and decisive action.

7. Use of Images and Video

The use of images, including photographs and videos, is a valuable aspect of teaching and learning that should be encouraged, provided there is no infringement of copyright or other rights. This encompasses images sourced from the internet as well as those belonging to staff or learners. Learners are required to consent to the use of their personal images upon enrolment.

It is important for all learners and staff to understand the risks associated with downloading and sharing these images online, especially when posting them on social networking sites. When learners intend to capture or utilise photographs or videos of individuals, whether learners or staff, they must obtain prior consent and clarify their intended use of the material.

Photographs or videos taken on our premises should be approached with care, ensuring that they do not include individuals' full names. Our goal is to promote best practices and provide additional guidance to all users on safeguarding their personal information.

8. Education and Training

Learners
WS Training emphasises the importance of balancing regulation and technical solutions with comprehensive learner education to foster responsible digital behaviour. E-safety education at WS Training includes:

- Promoting the 'Be E-aware – Connect with Care' campaign to raise awareness among learners about e-safety.
- Integrating e-safety into steps to success and apprentice inductions, incorporating activities like the Digital Resilience Framework and Safer Internet principles, aligned with the company's Acceptable Use Policy and available e-safety resources.
- Conducting e-safety sessions as part of the safeguarding unit within the PSHE curriculum during the initial term.
- Encouraging learners to understand and adhere to the Acceptable Use Policy, promoting safe and responsible IT use across all sites.
- Introducing learners to the parameters of blended learning, emphasising engagement and behavioural expectations through the Code of Conduct for learners and apprentices in Remote Learning.
- Reinforcing key e-safety messages throughout the curriculum delivery, focusing on critical awareness of online content, validation of information accuracy, and awareness of potential risks such as challenges, hoaxes, and unsafe activities on social media platforms.
- Highlighting the impact of inappropriate use on both individuals and the company, educating learners on how to report observed misuse and seek appropriate support.
- Stressing the importance of acknowledging information sources and respecting copyright when using internet-accessed materials.

- Supporting learners in developing positive and professional social media profiles through PSHE sessions and activities on Safer Internet Day to enhance their employability prospects.
- Training on identifying AI-generated misinformation and ethical AI use will be included in e-safety education.

Staff
It is essential that all staff understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An introduction to e-safety will be part of the safeguarding introduction for all new staff.
- A schedule of planned CPD activity to update staff will be provided by the DSL with responsibility for e-Safety and PREVENT – this training will be tailored appropriate to staff's role.
- CPD training will include awareness of AI risks and best practices in educational settings.
- The Designated Safeguarding Lead and the Safeguarding Team will receive updated and training and share these as relevant through e-safety updates in CPD sessions.

Parents/Carers
Parents/carers will be provided with guidance through the Parent Mail, to improve their understanding of online risks and strategies to keep their young person safe.

9. Security

The company is dedicated to ensuring network safety and security while meeting curriculum and administrative needs within available resources. Cybersecurity requires ongoing adaptation to address evolving threats.

Current Security Measures

- Firewall and Filtering: Internet firewall, Smoothwall website filtering.
- Software Protections: Anti-spam and anti-virus software with auto-updates.
- Access Control: Computer lockdowns to limit software installation and script execution, privileged access permissions, robust password policy, and Multi-Factor Authentication (MFA) for staff Remote Desktop access.
- Device Management: Segregation of learner BYOD (Bring Your Own Device).
- Smoothwall Monitoring System: Continuous network monitoring to detect and prevent inappropriate content access, safeguarding users and enhancing network security.

Cyber Essentials and Ongoing Security
The company aims to meet Cyber Essentials requirements for key administrative PCs and servers. Ongoing security efforts include:

- Regular reviews and updates.
- New backup systems.
- Enhanced patching solutions.

The safeguarding team will oversee the effectiveness of filtering systems.

Technical Infrastructure

- Management and Audits: IT systems are managed to meet e-safety requirements with regular safety and security audits.

- Physical Security: Servers, wireless systems, and cabling are securely located with restricted access.
- User Access: Users receive a username and password at enrolment or employment start, responsible for keeping login credentials secure.
- Filtering and Monitoring: Managed filtering service is maintained, with regular reviews of internet filtering categories. IT staff may monitor user activity as stated in the Acceptable Use Agreement.

Personal Information Management
WS Training Ltd ensures the safety and security of personal information, such as names, dates of birth, email addresses, and assessment materials, in line with GDPR legislation.

Data Security Responsibilities:
- Data Handling: Staff must safeguard learners' personal information, use password-protected devices, and ensure proper log off.
- Data Transfers: Encryption and secure devices are required for data transfers.
- Device Security: Company-owned mobile devices must be password-protected and signed out by IT/HR staff.
- Data Deletion: Personal data no longer required must be securely deleted according to the Company's Data Protection Policy.

10. Responding to Incidents

We expect all members of WS Training to use IT resources responsibly and follow this policy. However, policy breaches can occur due to carelessness, irresponsibility, or, in rare cases, deliberate misuse. Such incidents may lead to disciplinary actions for both staff and learners. It is essential for everyone to report any suspected or actual misuse, which may include:

- **Security Threats:** Any actions by staff or learners that compromise the safety and security of IT systems or users, violating the Acceptable Use Agreement.
- **Technical Failings:** Any discovered weaknesses in technical safeguards while using the systems and services.
- **Inappropriate Content:** Any incidents or access to messages or sites that make staff or learners feel uncomfortable or unsafe, such as cyberbullying, trolling, sexual harassment, or abuse (including the consensual and non-consensual sharing of nudes and revenge porn).
- **Equipment or Software Damage:** Any damage or faults involving equipment or software, regardless of how they occurred.

Reporting Misuse

- **Learners:** Report misuse to the DSL and Head of Education. Misuse will be addressed following the organisations Behaviour policy. Safeguarding issues must also be reported via MyConcern.
- **Staff:** Report misuse to the relevant site manager, who will notify HR and, if necessary, refer the matter to the Local Authority Designated Officer (LADO).

Handling Illegal Content

Upon discovering illegal content:

1. Do not touch the equipment or materials found.
2. Do not switch off computers or devices unless instructed by the Police.
3. Prevent further access to the illegal content by keeping others out of the area.
4. Do not view, download, print, or send any materials found, as this may result in further offences and personal liability for police investigation and prosecution.
5. Report all illegal content to the Police and the Internet Watch Foundation (www.iwf.org.uk).

Annex 1

Acceptable Use Policy (AUP)

Introduction

This Acceptable Use Policy (AUP) outlines the standards for the use of IT systems, networks, and digital resources for post-16 education institutions in the UK. The policy aims to ensure that all users, including staff and learners, act responsibly and ethically when using the organisation's IT facilities. Compliance with this policy is mandatory for all learners, staff, and visitors.

Scope

This policy applies to:

- All users of the company's IT systems, including learners, staff, and visitors.
- All IT equipment, networks, software, and data used within the organisation or remotely via company access.

General Principles

Respect and Responsibility

- Users must respect the rights and privacy of others and act responsibly when using IT resources.
- Users are responsible for their actions and activities involving IT systems and must comply with all relevant laws, regulations, and institutional policies.
- AI-generated content must be used responsibly. Users must not use AI tools to generate misleading, inappropriate, or unethical material.

Appropriate Use

- IT resources must be used for educational, research, and administrative purposes only.
- Personal use of IT resources should be limited and must not interfere with company activities or violate any policy.
- Users must not submit AI-generated work as their own unless explicitly permitted by staff.

User Responsibilities

Account Security

- Users must use their own accounts and are responsible for maintaining the security of their login details, which will be generated and managed by Unite Networks.
- Users must not share their login details with others.

Data Protection

- Users must comply with data protection laws, ensuring that personal and sensitive data is stored, processed, and transmitted securely.
- Personal data must be used only for the purpose for which it was collected and should not be disclosed without proper authorisation.
- Users must not input personal, sensitive, or confidential data into AI tools unless explicitly authorised by the organisation.

Respect for IT Systems

- Users must not attempt to damage or disrupt IT systems, networks, or data.
- Unauthorised access, modification, or use of the company's IT resources is strictly prohibited.
- AI-powered tools that automate interactions, modify content deceptively, or bypass security measures are not permitted.

Prohibited Activities

Inappropriate Content

- Users must not access, download, store, or transmit any content that is illegal, offensive, discriminatory, or harmful.
- Cyberbullying, harassment, and any form of online abuse are strictly prohibited.
- AI must not be used to create, distribute, or manipulate harmful or deceptive content, including deepfakes or misinformation.

Software and Licensing

- Only software authorised by the company should be installed and used on company IT equipment.
- Users must not use or distribute pirated or unlicensed software.

Network Security

- Users must not engage in activities that compromise network security, such as hacking, phishing, or spreading malware.
- The use of personal devices on the company's network must comply with BYOD (Bring Your Own Device) security guidelines.
- AI-related cybersecurity risks, including AI-generated phishing attempts and automated cyber threats, will be monitored and mitigated by IT security protocols.

Monitoring and Enforcement

Monitoring

- The company reserves the right to monitor IT systems and network traffic to ensure compliance with this policy and to maintain a safe digital environment.
- Monitoring will be conducted in strict accordance with relevant privacy laws and company policies, ensuring respect for individual privacy within the bounds of safeguarding responsibilities.

- The company uses Smoothwall monitoring software to flag inappropriate searches, prevent access to harmful or inappropriate content, and promptly identify potential security threats. This proactive approach enhances both online safety and security.
- Smoothwall monitors all learner laptops and staff laptops that have direct contact with learners. Monitoring is limited to relevant devices and does not extend to staff laptops used by those without direct contact with learners.
- Alerts generated by Smoothwall will be reviewed by the Designated Safeguarding Lead, and in her absence be reviewed by the CEO only, who will take appropriate action in line with safeguarding policies and escalate any serious concerns as necessary.
- Regular audits of Smoothwall's monitoring effectiveness will be conducted to ensure ongoing alignment with company policies, safeguarding requirements, and current cybersecurity standards.
- AI-generated content and interactions may be monitored to ensure compliance with this policy. Where necessary, AI detection tools may be used to uphold academic integrity.

Enforcement

- Violations of this policy may result in disciplinary action, including suspension or termination of access to IT resources, and in serious cases, legal action.
- Users are encouraged to report any suspected violations of this policy to the DSL/Safeguarding team or Unite Networks.

Acknowledgment

By using the company's IT systems, users acknowledge that they have read, understood, and agree to comply with this Acceptable Use Policy.