Online Safety Policy

| Version 2.0 |

Policy Commencement Date	10/08/2026
Policy Version	2.0
Review by	09/8/2027
Document Controller	Jonathan Hall
Signature	*J.Hall*

Contents page

Content	Page
1. Introduction	3
2. Scope	3
3. Key Legislation and Guidance	4
4. Key Pillars of the Online Safety Policy	4
5. Roles and Responsibilities	4
6. Acceptable Use of Technology	4
7. Managing Online Risks	5
8. Reporting a Concern	5
9. Policy Review	10
10. Related Policies and Procedures	10

Version 2.0 Summary of Changes

The Online Safety Policy has been comprehensively reviewed and strengthened to reflect current safeguarding expectations, emerging online risks, and best practice guidance. Key changes include:

- Introduction of a definitions section to provide clarity on key online safety terminology.
- Expansion of reporting procedures, including incident management, escalation processes, record keeping, and support arrangements.
- Addition of a dedicated Filtering and Monitoring section outlining organisational controls, responsibilities, and review arrangements.
- Introduction of Online Safety Training and Awareness requirements for staff and learners.
- Addition of a Learner Online Safety Education section to promote digital resilience, safe online behaviour, and responsible technology use.
- Inclusion of Emerging Online Risks guidance covering artificial intelligence (AI), misinformation, online scams, social media risks, and manipulated digital content.
- Strengthening of safeguarding and Prevent-related procedures through more detailed operational guidance and referral pathways.
- Addition of a Related Policies and Procedures section to improve alignment with the wider organisational policy framework.

Overall, Version 2.0 expands the policy from a high-level framework into a more comprehensive and operational document, enhancing online safeguarding, staff accountability, learner protection, and organisational compliance.

1. Introduction

1.1 This policy outlines the procedures and guidance for ensuring the online safety of all learners and staff at Staff Power Training (SPT). Our aim is to create a safe and respectful online environment that allows for effective learning while protecting individuals from potential harm. It has been developed in line with key national guidance, including the UK government's "Keeping Children Safe in Education" and best practice recommendations from the UK Safer Internet Centre.

2. Scope

2.1 This policy applies to all learners, staff, contractors, and visitors using the SPT IT systems, whether on-site or remotely.

For the purposes of this policy:

Online Safety
The safe and responsible use of digital technologies, online services, internet-connected devices, and communication platforms to protect individuals from harm and promote positive online experiences.

Cyberbullying
Any form of bullying, harassment, intimidation, or threatening behaviour carried out through digital technologies, including social media, messaging services, email, online gaming platforms, or other electronic communication methods.

Harmful Content
Any online material that may cause physical, emotional, psychological, or reputational harm to an individual, including abusive, discriminatory, violent, extremist, misleading, or illegal content.

Online Grooming
The process by which an individual establishes a relationship with a child, young person, or vulnerable adult online with the intention of manipulating, exploiting, or abusing them.

Radicalisation
The process through which an individual comes to support extremist ideologies, beliefs, or activities that may lead to harm or criminal behaviour.

Filtering
Technical measures used to restrict access to inappropriate, illegal, or potentially harmful online content whilst supporting legitimate educational and business activities.

Monitoring
The review and analysis of network activity, systems, and online behaviour to identify safeguarding concerns, security threats, misuse of systems, or breaches of organisational policies.

Personal Data
Any information relating to an identified or identifiable living person, as defined under UK GDPR.

3. Key Legislation and Guidance

3.1 This policy is written in accordance with:

- Keeping Children Safe in Education (KCSIE)
- The Prevent Duty
- UK General Data Protection Regulation (UK GDPR)
- Guidance from the UK Safer Internet Centre and the NSPCC

4. Key Pillars of the Online Safety Policy

4.1 The policy is built around a commitment to four key principles:

- Empowerment: Equipping learners and staff with the knowledge and skills to use technology safely and responsibly.
- Protection: Implementing technical and procedural safeguards to protect users from online harm.
- Inclusion: Ensuring that all members of our community can access online resources and support without fear of discrimination or harassment.
- Accountability: Establishing clear roles, responsibilities, and reporting mechanisms to address any online safety incidents effectively.

5. Roles and Responsibilities

SPT has designated a clear structure of responsibility for online safety:

5.1 Designated Safeguarding Lead (DSL): The DSL will have overall responsibility for online safety, leading on policy implementation, staff training, and managing any reported concerns.

5.2 IT Department: The IT department will ensure the security of the provider's network and systems, including appropriate filtering and monitoring.

5.3 Tutors and Assessors: All teaching staff are responsible for promoting online safety within their sessions, modelling good practice, and identifying and reporting any concerns.

5.4 Learners: Learners are expected to adhere to the acceptable use policy and report any online safety concerns they may have for themselves or others.

6. Acceptable Use of Technology

6.1 The policy provides clear guidelines on the acceptable use of the training provider's IT systems, including the use of email, internet, social media, and personal

devices. This includes strict prohibitions on:

- Accessing, creating, or distributing offensive, illegal, or discriminatory material.
- Cyberbullying, harassment, or any form of online abuse.
- Infringing copyright and intellectual property rights.
- Attempting to bypass security measures.

7. Managing Online Risks

SPT recognise the diverse range of online risks, this policy details specific measures to mitigate them. These include:

7.1 Filtering and Monitoring: Appropriate and proportionate filtering and monitoring systems will be in place to block access to harmful content.

7.2 Data Protection: All personal data will be handled in accordance with UK GDPR, and learners will be educated on how to protect their own personal information online.

7.3 Online Communication: Clear guidance is provided on professional and safe communication between staff and learners, including the use of approved platforms.

7.4 Cyberbullying: SPT have a zero-tolerance approach to cyberbullying. Any incidents will be investigated and may result in disciplinary action.

7.5 Radicalisation and Extremism: The policy addresses the risk of online radicalisation, in line with the Prevent duty, and provides clear reporting pathways.

8. Reporting a Concern

8.1 Any learner or member of staff who has an online safety concern can report it to any member of staff, who will then escalate it to the Designated Safeguarding Lead. All reports will be taken seriously, investigated promptly, and dealt with in a confidential and supportive manner. SPT is committed to responding promptly and effectively to all online safety concerns. Any concerns relating to online safety, cybersecurity, cyberbullying, harmful content, inappropriate online behaviour, radicalisation, or safeguarding risks must be reported immediately using the below process:

- Learners, staff, contractors, and visitors should report any online safety concern to a member of staff as soon as possible.
- Staff receiving a concern must immediately inform the Designated Safeguarding Lead (DSL).
- Any immediate risk of harm must be escalated without delay in accordance with the Safeguarding Policy.
- All concerns will be treated seriously and handled confidentially wherever possible.

Managing an Incident

Upon receipt of a report, the DSL will:

1. Assess the nature and severity of the concern.

2. Record the incident using the organisation's safeguarding reporting procedures.
3. Determine whether additional evidence should be preserved, including screenshots, emails, or system logs.
4. Identify whether the concern constitutes a safeguarding matter, disciplinary issue, data breach, or criminal offence.
5. Take appropriate action to safeguard those affected.
6. Refer concerns to external agencies where required, including the Local Authority, Police, Prevent partners, Internet Watch Foundation, or other relevant organisations.

Recording and Reviewing Incidents

- All online safety incidents will be documented and retained in accordance with data protection requirements.
- Records will include actions taken, outcomes, referrals made, and any lessons learned.
- Trends and recurring concerns will be reviewed periodically to identify opportunities for improvement and additional training.

Support for Those Involved

SPT will provide appropriate support to learners and staff affected by online safety incidents. This may include safeguarding interventions, welfare support, referral to external agencies, or additional guidance on staying safe online.

Learning from Incidents

Where appropriate, incidents will be reviewed by the DSL and senior management to identify lessons learned and any improvements required to policies, procedures, training, filtering, monitoring, or safeguarding arrangements.

8.2 If required online safety concerns can also be reported via the UK Safer Internet Centre - Report Harmful Content:
https://reportharmfulcontent.com/harms

Filtering and Monitoring

SPT is committed to maintaining appropriate and proportionate filtering and monitoring arrangements to help safeguard learners, staff, and organisational systems from online harm. Filtering and monitoring measures are designed to prevent access to inappropriate content, identify potential safeguarding concerns, and support a safe online learning environment.

Filtering

SPT will implement suitable internet filtering controls to reduce the risk of users accessing harmful, illegal, extremist, abusive, or otherwise inappropriate online content. Filtering arrangements will be regularly reviewed to ensure they remain effective, proportionate, and appropriate to the needs of learners and staff.

Access to blocked content for legitimate educational or business purposes may be permitted following approval from authorised personnel. Any attempts to circumvent or bypass filtering controls may be investigated and managed in accordance with organisational policies and procedures.

Monitoring

SPT reserves the right to monitor the use of its IT systems, networks, devices, internet access, and approved communication platforms to help safeguard users, protect organisational assets, and ensure compliance with legal and policy requirements. Monitoring will be conducted in a lawful, proportionate, and transparent manner and in accordance with UK GDPR requirements.

Monitoring activities may identify indicators of:

- Access to inappropriate or harmful content.
- Cyberbullying, harassment, or online abuse.
- Attempts to bypass security controls.
- Potential safeguarding concerns.
- Radicalisation or extremist activity.
- Cybersecurity threats or unauthorised system use.

Roles and Responsibilities

The IT Department is responsible for maintaining filtering and monitoring systems and ensuring they remain operational and effective. The Designated Safeguarding Lead (DSL) will review and manage any safeguarding concerns identified through monitoring activities and ensure appropriate action is taken where required. Senior management will maintain oversight of filtering and monitoring arrangements and review their effectiveness on a regular basis.

Review of Arrangements

Filtering and monitoring arrangements will be reviewed at least annually, or sooner following significant incidents, changes in legislation, or changes to organisational systems and risks. Any identified weaknesses will be addressed promptly to ensure continuous improvement of online safety arrangements.

Online Safety Training and Awareness

SPT recognises that effective online safety relies upon staff and learners understanding the risks associated with the use of digital technologies and knowing how to respond appropriately to concerns. Online safety awareness forms an important part of the organisation's safeguarding culture.

Staff Training

All staff will receive online safety training as part of their induction and through regular safeguarding updates. Training will be appropriate to individual roles and responsibilities and will include:

- Recognising online safety risks and concerns.
- Cyberbullying and online harassment.
- Safe use of digital devices and communication platforms.
- Data protection and information security.
- Online radicalisation and the Prevent Duty.
- Reporting and responding to online safety incidents.
- Emerging online risks and technologies.

The Designated Safeguarding Lead (DSL) and other safeguarding personnel will undertake additional training relevant to their responsibilities and maintain an up-to-

date understanding of online safeguarding risks and best practice.

Learner Awareness
Learners will be provided with guidance and support to help them use technology safely, responsibly, and respectfully. Online safety awareness may be delivered through induction activities, tutorials, training sessions, safeguarding communications, and other learning opportunities. Topics may include:

- Safe use of social media and online platforms.
- Protecting personal information online.
- Recognising scams, fraud, and phishing attempts.
- Reporting concerns and seeking support.
- Appropriate online behaviour and digital citizenship.
- Recognising harmful or inappropriate content.

Review and Continuous Improvement
Online safety training and awareness activities will be reviewed regularly to ensure they reflect current legislation, emerging risks, organisational needs, and recognised safeguarding best practice.

Learner Online Safety Education
SPT is committed to helping learners develop the knowledge, skills, and confidence required to participate safely and responsibly in the online environment. Online safety education forms an integral part of the learner experience and supports the organisation's wider safeguarding responsibilities.

Promoting Safe Online Behaviour
Learners will be encouraged to:

- Use digital technologies responsibly and respectfully.
- Protect their personal information and online identity.
- Think critically about information encountered online.
- Treat others with dignity and respect in all online interactions.
- Report any concerns relating to online safety, cyberbullying, or harmful content.

Online Safety Awareness
SPT will provide learners with guidance and information on a range of online safety topics, including:

- Safe use of social media and online communication platforms.
- Protecting personal information and privacy settings.
- Recognising scams, phishing, and online fraud.
- Cyberbullying and online harassment.
- Digital wellbeing and managing online activity responsibly.
- Identifying misinformation and disinformation.
- Risks associated with extremist content and online radicalisation.
- Safe use of emerging technologies, including artificial intelligence (AI).

Access to Support
Learners who experience online safety concerns will be encouraged to seek support from tutors, assessors, safeguarding staff, or the Designated Safeguarding Lead (DSL). Appropriate advice, guidance, and safeguarding support will be provided where required.

Building Digital Resilience
SPT aims to support learners in developing digital resilience by promoting critical thinking, responsible decision-making, and an understanding of the potential risks and benefits associated with online activities. Learners will be encouraged to challenge inappropriate behaviour and contribute to a safe and inclusive online learning environment.

Emerging Online Risks
SPT recognises that technology and online behaviours continue to evolve, creating new opportunities as well as potential risks. The organisation is committed to maintaining awareness of emerging online threats and adapting its safeguarding arrangements accordingly.

Artificial Intelligence (AI)
Learners and staff may use artificial intelligence tools to support learning and work activities. Users should exercise caution when using AI-generated content and should:

- Verify the accuracy of information generated by AI systems.
- Avoid sharing confidential, personal, or sensitive information with AI platforms unless authorised to do so.
- Use AI technologies responsibly, ethically, and in accordance with organisational policies.
- Understand that AI-generated content may contain inaccuracies, bias, or misleading information.

Misinformation and Disinformation
SPT encourages learners and staff to critically evaluate information obtained online and from social media platforms. Users should be aware that false, misleading, or manipulated content may be presented as factual information and should utilise trusted sources when researching or sharing information.

Online Scams and Fraud
Learners and staff should remain vigilant to the risks of online scams, phishing attempts, identity theft, and financial fraud. Suspicious emails, messages, websites, or requests for personal information should be reported in accordance with organisational procedures.

Social Media Risks
While social media can support communication and engagement, users should be aware of the potential risks associated with inappropriate content, cyberbullying, privacy breaches, misinformation, and reputational damage. All users are expected to conduct themselves professionally and respectfully when engaging online.

Manipulated and Synthetic Content
The increasing availability of digitally altered images, videos, audio recordings, and other synthetic content can make it difficult to distinguish between genuine and fabricated material. Learners and staff should exercise caution when assessing the authenticity of online content and report any material that may cause safeguarding concerns.

Continuous Review
SPT will monitor developments in technology and emerging online risks and will update its policies, procedures, training, and awareness activities as required to maintain an effective online safety framework.

9. Policy Review
9.1 This policy will be reviewed annually, or more frequently if there are significant changes in legislation, working practices, or following any related incidents.

10. Related Policies and Procedures
This policy should be read in conjunction with other organisational policies and procedures that contribute to safeguarding, security, and the wellbeing of learners and staff. These include:

- Safeguarding and Child Protection Policy
- Prevent Duty Policy
- Data Protection Policy
- Information Security Policy
- Acceptable Use of IT Policy
- Staff Code of Conduct
- Learner Code of Conduct
- Equality, Diversity and Inclusion Policy
- Disciplinary Policy
- Whistleblowing Policy
- Complaints Policy

Where an online safety concern involves a safeguarding risk, staff must follow the organisation's Safeguarding and Child Protection Policy and associated reporting procedures. Concerns relating to data breaches, information security incidents, or inappropriate conduct may also be managed in accordance with the relevant organisational policies and procedures.