SPS The UK School of Professional Studies

Online Safety Policy

Version	1.0
Date last updated:	July 2025
Next update:	July 2026
Category	Regulations
Document Owner:	Dean
Publication:	Public

Contents

1. Purpose

1.1. This Online Safety Policy sets out how the organisation protects learners, staff and visitors from online risks, promotes safe and responsible use of digital technologies, and ensures that all aspects of online delivery are conducted in a secure, professional and safeguarding-focused manner. The policy supports our wider safeguarding responsibilities, including compliance with the Prevent Duty, Data Protection requirements, and expectations for safe and effective online learning.

1.2. Its purpose is to ensure that everyone involved in our programs understands their responsibilities in preventing harm, recognising online risks, and reporting concerns promptly.

2. Scope

2.1. This policy applies to all Learners, Staff, Contractors, Partner Organisations, Visiting Speakers and any individuals engaging with our training provision, whether in person or online.

2.2. It covers the safe use of all digital and online tools associated with learning, such as:

- virtual classrooms and video-conferencing platforms
- learning management systems and assessment platforms
- communication tools such as email, chat functions and discussion forums
- social media used in connection with learning
- AI tools, coding environments or digital resources used during training
- any personal devices used to access course content or communicate with staff or other learners

2.3. The scope includes risks arising from online communication, cyberbullying, exposure to extremist or harmful content, scams and fraud, safeguarding disclosures made online, data security, and inappropriate or unsafe online behaviour.

3. Roles and Responsibilities

3.1. A safe and secure online learning environment relies on all members of the School of Professional Studies (SPS) understanding their duties. The following roles outline how online safety is managed, monitored and promoted across our provision.

3.2. **Designated Safeguarding Lead (DSL)** - The DSL oversees institutional policy to ensure compliance with regulation and legislation, that it reflects best practice in the sector, and that it is effectively implemented. Additionally, they provide training, liaise with external agencies, oversees disclosures, and are responsible for reporting through the governance system.

3.3. **Senior Management Team** – They provide strategic oversight of online safety across the organisation, ensuring this policy is implemented, reviewed annually and aligned with safeguarding, Prevent and data protection requirements. They allocate sufficient resources for staff training, secure digital systems and safe online delivery, ensuring all staff understand how to identify and respond to online risks.

3.4. **Tutors, Trainers and Assessors** – Promote safe and respectful online behaviour in all learning environments and follow organisational procedures for secure remote delivery (e.g., use of breakout rooms, recording consent, supervision). They will monitor learner behaviour in online sessions and report concerns immediately to the DSL. They will ensure that learning materials, platforms and digital resources used are safe, appropriate and compliant with policy.

3.5. **Support Staff, Administrators and Technical Staff** –Maintain secure digital systems, platforms and access controls. Report any breaches, suspicious activity or technical concerns to the DSL. Ensure new learners receive induction materials related to online safety and data protection and support learners who require help accessing online platforms safely.

3.6. **Learners** – Must use digital tools, platforms and communication channels in a respectful, responsible and lawful manner. Protect their own personal information and follow all instructions relating to passwords, device security and safe behaviour online. Report any concerns, suspicious activity or inappropriate behaviour they encounter online.

3.7. **External Partners, Contractors and Visiting Speakers** – Must comply with this Online Safety Policy and use only approved platforms and communication channels when working with learners. They will report safeguarding or online safety concerns promptly to the DSL.

4. Acceptable Use

General Expectations

4.1. All learners and employees will be assigned a personal IT user account with specific login credentials (i.e., username and password), which can be used to log on to any computer connected to the SPS network. A person's IT user account is for their use only; employees and learners should take all reasonable steps to prevent unauthorised use of their user account by anyone other than themselves.

4.2. All users must:

- Use online systems in a respectful, lawful and professional manner.
- Ensure communication (verbal, written, chat, email or video) is appropriate and related to learning or organisational activity.
- Protect login details and never share passwords or access information with others.
- Access online platforms only through personal accounts provided or approved by SPS
- Immediately report any technical issues, suspicious activity, security breach, or safeguarding concern.

Use of Devices

4.3. Users must:

- Ensure personal or organisational devices used for training are safe, secure and protected with passwords or biometric locks.
- Keep devices updated with current operating system and security patches.
- Avoid using public or unsecured Wi-Fi when accessing confidential or sensitive information.
- Not attempt to access, modify or interfere with systems, accounts or networks they are not authorised to use.

Behaviour in online sessions

4.4. During live online teaching or meetings, users must:

- Treat others with courtesy and respect at all times.
- Follow tutor instructions regarding cameras, microphones and chat functions.

- Dress appropriately and ensure backgrounds (virtual or physical) are suitable for a professional learning environment.
- Not record, screenshot or share any part of a session unless explicit permission has been granted by SPS
- Use chat functions responsibly and avoid offensive or disruptive comments

Use of Messaging, Email and Digital Communication Tools

4.5. Users must:

- Use organisational communication channels for learning-related communication.
- Keep interactions with Staff and Learners professional and appropriate.
- Not share or distribute any content that is abusive, discriminatory, extremist, threatening, explicit or otherwise harmful.
- Not engage in or encourage cyberbullying, harassment or intimidation.

Social Media Use

4.6. When using social media in connection with learning or representing the organisation, users must:

- Behave respectfully and avoid posting content that could damage SPS reputation.
- Not connect with staff or learners on personal social media accounts unless approved for professional use.
- Not share confidential information, screenshots, learning materials or assessment content online.

4.7. SPS acknowledges the role of social media in the proliferation of extremist views and the radicalisation of vulnerable individuals. SPS may monitor, record, and block, the use of social media sites and apps where it considers there is risk that a person has been radicalised or drawn into terrorism. In determining whether content viewed, shared or posted falls under this category SPS will consider:

- whether there are any indications that the person is supportive of terrorism, violent extremism, or is espousing hateful/harmful views that may suggest that they are vulnerable to radicalisation

- whether there is any clear trigger – whether comments, or patterns of behaviour, or evidence of engagement with harmful material – that would justify intervention, Posting, sharing, or downloading terrorist or extremist materials may be a criminal offence under the Counter Terrorism and Security Act 2015 and SPS will cooperate fully with the authorities when required to do so

Use of AI, Coding Tools and Digital Resources

4.8. Where AI tools, coding platforms or digital assistants are used as part of the programme:

- Users must ensure outputs are safe, appropriate and checked for accuracy.
- AI-generated content must not be used to plagiarise assignments or assessments.
- Any harmful, explicit or extremist content generated or encountered must be reported immediately.
- Tools should only be accessed through safe, approved platforms and within course guidelines.

Consequences of breaching acceptable use

4.9. Breaches of this policy may result in:

- Removal of access to SPS systems.
- Disciplinary action (staff) or removal from programme (learners).
- Referral to external agencies where behaviour constitutes a safeguarding or criminal concern.

5. Risk Assessment

5.1. We recognise that online learning and the use of digital technologies introduce specific safeguarding, security and wellbeing risks. SPS assesses these risks regularly to ensure all learners and staff are protected.

5.2. Our risk assessment considers factors such as remote delivery, the use of personal devices, interaction on digital platforms, exposure to harmful or inappropriate content, cybercrime, scams, and the potential for extremist or radicalising material to be accessed online.

5.3. We review risks at programme design stage and throughout delivery, updating our procedures as new technologies, threats or safeguarding concerns emerge. Identified risks are managed through staff training, secure platform selection, robust access controls, clear behaviour expectations and effective reporting routes.

6. Safe Remote Teaching and Online Delivery

6.1. SPS is committed to ensuring that all remote and online learning is delivered safely, securely and in line with safeguarding expectations. All online sessions are conducted through approved platforms with appropriate security settings, such as waiting rooms, controlled screen-sharing and restricted access links. Tutors are responsible for maintaining a professional, safe learning environment by monitoring learner behaviour, managing chat functions and reporting any concerns immediately.

6.2. Learners must follow guidance on appropriate conduct during remote sessions, including using suitable backgrounds, behaving respectfully and not recording or sharing content without permission. Identity verification is carried out where required, and all digital interactions between staff and learners must take place through authorised channels. Our procedures are reviewed regularly to ensure emerging risks in online delivery are identified and addressed promptly.

7. Prevent Duty and Online Extremism

7.1. SPS recognises that online platforms can expose learners to extremist, radicalising or otherwise harmful content. In line with the Prevent Duty, we take proactive steps to reduce these risks and promote a safe, inclusive learning environment. Staff are trained to identify early indicators of radicalisation, extremist views or concerning online behaviour and must report any concerns immediately to the DSL.

7.2. We use secure, approved digital platforms and monitor online interactions to ensure learners are not exposed to extremist material during training. Learners are encouraged to think critically, challenge misinformation and report any content that makes them feel unsafe. Any Prevent-related concerns are managed in line with safeguarding procedures and, where appropriate, referred to external agencies for further support.

8. Use of AI and Digital Tools

8.1. SPS recognises the growing role of artificial intelligence, coding assistants and other digital tools in teaching and learning. While these technologies can enhance learning, they also introduce risks related to accuracy, misuse, safeguarding and data security. To ensure safe and responsible use, learners and staff must only access AI or digital tools through approved platforms and for legitimate learning purposes.

8.2. All users are expected to critically evaluate AI-generated content and must not use AI tools to engage in plagiarism, produce misleading information or complete assessments dishonestly. Any output from AI systems that is harmful, explicit, discriminatory or otherwise inappropriate must be reported immediately to the DSL. Staff are responsible for guiding learners in the safe, ethical and responsible use of these tools and for ensuring that no personal or sensitive data is entered into AI systems without authorisation.

8.3. SPS reviews emerging digital technologies regularly and updates its procedures to ensure that the use of AI and related tools supports learning safely, ethically and in line with safeguarding requirements.

9. Monitoring and Reporting a Concern

9.1. SPS maintains oversight of online activity to ensure a safe and secure digital learning environment. Approved platforms may be monitored to identify inappropriate behaviour, safeguarding risks, security breaches or misuse of systems. Monitoring is carried out in a proportionate way and in line with data protection requirements.

9.2. All staff and learners share responsibility for recognising and reporting online safety concerns. Any incident involving harmful content, suspicious behaviour, cyberbullying, extremist material, misuse of technology or a safeguarding disclosure must be reported immediately to the DSL. Staff must report to the DSL without delay, record concerns accurately and never investigate issues independently.

9.3. Serious or repeated concerns may be escalated to external safeguarding partners, Prevent teams or law enforcement where appropriate. Learners are encouraged to report anything that makes them feel unsafe online, and all reports are handled sensitively and in line with *Safeguarding and Prevent Policy.*

10. Training and Induction

10.1. SPS ensures that all staff and learners receive appropriate training and guidance to promote safe and responsible online behaviour. Staff are provided with regular training on online safety, safeguarding, Prevent Duty requirements, cyber awareness, and the safe use of digital platforms used within the organisation.

10.2. Tutors delivering online or blended learning receive additional guidance to help them identify risks, manage online behaviour and respond effectively to concerns.

10.3. All learners receive an online safety induction at the start of their program. This includes guidance on safe use of digital tools, recognising online risks such as scams, misinformation or extremist content, and understanding expected behaviour during online sessions. Learners are shown how to report concerns and where to access support.

10.4. Training needs are reviewed regularly, and refresher updates are provided to ensure everyone remains aware of emerging risks, new technologies and changes in safeguarding procedures.

11. Policy Review

11.1. This Policy will be reviewed and updated on an annual basis.

Version History

Version	Changes	Date	Approved by:
0.1	Draft	-	-
1.0	First approved version	July 2025	Governing Body