Online Safety Policy 2026/2027

Policy Author	Samantha Collins
Approved by	Jamie Crinigan
Position	Managing Director
Approved date	October 2027
Signed	S.Collins
Next review date	August 2027
Version	2

I. Introduction

Skills4 is committed to providing a safe and secure environment in which both learners and staff can flourish, and this is reflected in our safeguarding processes. This policy has been written to provide clear guidance to ensure that this commitment is embedded into the culture and ethos of the company. It is therefore essential that all staff are aware of their duties regarding online safety and report any concerns promptly.

The Designated Safeguarding Lead is referred to as the DSL, and the Deputy Designated Safeguarding Lead is referred to as the DDSL within this policy.

Name	Role
Jamie Crinigan	MD with overall accountability for Safeguarding and Prevent.
Barbara Van der Eecken	Chair of Safeguarding Sub-Committee (SSC)
Sam Collins	Designated Safeguarding Lead (SSC member)
Victoria England	Deputy Designated Safeguarding Lead (SSC member)
Claire Chidlow	Deputy Designated Safeguarding Lead and named Prevent Lead (SSC member)
Rehana Khan	HR Lead for Safer Recruitment
John Norton	Safeguarding and Inclusion Lead (SSC member)

II. Purpose

This policy outlines Skills4's approach to online safety in accordance with best practice in the FE education sector. It provides guidance to staff on online and technology-based communications with learners and colleagues.

III. Introduction

This policy applies to all members of staff and learners who have access to Skills4's IT systems, including Microsoft Teams, whether on the premises or working remotely. It applies to all use of the internet and electronic communication devices, including email, mobile phones, video conferencing, social media and messaging services, online games, and any other systems that use the internet for communication and information storage. This policy also emphasises the importance of keeping learners safe online, both at home and at work. It ensures that all users are aware of the potential risks associated with online activity and provides guidance on the safe and responsible use of digital tools and resources to protect the wellbeing of all users in online environments.

IV. Aim

Skills4 recognises that social media and other forms of technology provide excellent learning opportunities but also create significant risks. Given the online delivery and communication tools used by Skills4, it is crucial that staff and learners use this technology responsibly, with clear policies in place to support and encourage responsible use. As part of our statutory duty, Skills4 is committed to safeguarding and promoting the safety and welfare of children, young people and vulnerable adults. This is achieved through a combination of security measures, training, guidance, and the implementation of the Prevent and Radicalisation Policy and Prevent risk assessment and action plan.

Our approach integrates the principles of the Prevent duty, aiming to protect individuals from being drawn into extremism and radicalisation. We implement robust safeguards and support mechanisms to empower staff and learners to identify and manage risks appropriately.

The key mechanisms for ensuring that information about online safety is delivered, checked and reinforced include:

- Learner and apprentice induction
- Group tutorials
- Guidance and materials provided for learner self-access, for example via Bud and SharePoint
- Progress review meetings
- Online teaching and learning sessions

This Online Safety Policy outlines how technology can be used for the professional benefit of both staff and learners at Skills4.

Skills4 would like to ensure that members of staff follow the same professional standards online as they would in real life, including those who are required to follow the GPhC standards for Pharmacy Professionals or General Dental Council standards.

This Online Safety Policy should be read in conjunction with the Safeguarding Policy, Keeping Children Safe in Education 2026, the Internet, Email and Social Media Usage Policy and Guidelines, the Prevent and Radicalisation Policy, and the Prevent risk assessment and action plan. Any member of staff found to be in breach of these policies and plans may be subject to disciplinary processes. This supports compliance with Skills4's broader safeguarding duties, including those associated with online safety, information security, filtering and monitoring, and the Prevent strategy.

V. Roles and Responsibilities

Learners will:

- Be provided with information on how to use the internet and other digital technologies both safely and responsibly.

- Be provided with information on how to use the internet and other digital technologies to support, extend and enhance their learning, including by accessing online learning sessions and materials via Bud.
- Develop an understanding of intellectual property and copyright.
- Develop skills to effectively use the internet for evidence-based research purposes and to avoid misinformation.
- Develop skills to evaluate information found online.
- Be shown how to report online safety concerns to their tutor or a member of the Welfare Team.
- Be educated on how to keep themselves safe online, with a focus on identifying vulnerabilities, recognising potential threats, and understanding what to watch for when attempts are made to influence or manipulate them through online platforms.
- Learn strategies to protect personal information and privacy while using digital technologies, ensuring that sensitive data is not shared or exposed online.
- Not access any prohibited content, in line with the IT Usage Policy.

Tutors will:

- Ensure that learners have the information they need to access online learning safely.
- Ensure that learners know what to do if they have a concern about online safety or online material.
- Work with learners to develop an understanding of how to access, evaluate, research and use online tools safely.

Leaders and managers will:

- Ensure that information about online safety is available to all staff and learners and reflects current Keeping Children Safe in Education 2026 expectations.
- Ensure that support and guidance on safe use of IT is provided to all staff, particularly with use and implementation of the Internet, Email and Social Media Usage Policy and Guidelines.
- Ensure that Skills4 IT equipment is maintained to a safe standard.
- Ensure that measures are in place to keep data safe and secure, restrict access to unsuitable content and provide appropriate filtering and monitoring across Skills4 systems, devices and relevant online learning environments in line with the Internet, Email and Social Media Usage Policy and Guidelines.

Employers (where relevant) will:

- Ensure that they are in full compliance with The Online Safety Act 2023.

All staff:

- Are responsible for ensuring the safety of learners.
- Should report any concerns immediately to their line manager or to a member of the Welfare Team in line with the Safeguarding Policy.

- When informed about an online safety incident, staff must take particular care not to guarantee any measure of confidentiality to the individual reporting it or to those involved.
- Should model safe, responsible and professional behaviours in their own use of technology at Skills4 and in their personal use.
- Ensure compliance with associated policies and risk assessments, including the Safeguarding Policy, Prevent and Radicalisation Policy, Prevent risk assessment and action plan, and online safety, filtering and monitoring arrangements.
- Remain professionally curious about online safeguarding risks, including cyberbullying, harmful sexual behaviour, online exploitation, radicalisation, misinformation, AI-generated content and any technology-facilitated abuse or harassment.

VI. Learner conduct

Learners must abide by the rules and values of Skills4, respecting the rights of fellow learners and staff, as well as the reputation of the organisation. It is essential that learners refrain from posting comments on social media or online, or sending text or other online messages that breach learner expectations, especially those that:

- Are unlawful.
- Could be viewed as bullying or harassing another member of the Skills4 community.
- Are contrary to equality, diversity and inclusion principles.
- Explicitly encourage others to break the law.
- Are likely to bring Skills4 into disrepute.

These guidelines are critical not only for maintaining a respectful and professional learning environment but also for aligning with Skills4's commitment to safeguarding and the Prevent duty. Safeguarding includes protecting learners from harm, abuse and exploitation and is closely linked with the Prevent duty, which aims to safeguard individuals from being drawn into extremism and radicalisation.

Posting content that could incite unlawful behaviour, promote harmful ideologies, or contribute to radicalisation is strictly prohibited. Such actions pose a significant risk to the safety and wellbeing of the learning community and are contrary to the safeguarding principles upheld by Skills4. For example, learners are also reminded not to post photos of a sexual nature. Any such incidents must be reported to the Welfare Team as part of our comprehensive safeguarding processes.

Additionally, learners should not attempt to contact or communicate with staff members via social networks, including attempting to add a member of staff as a 'friend.' Maintaining these professional boundaries supports our safeguarding framework, which also includes preventing the risk of radicalisation.

If a learner has any concern regarding the use of the internet or social media, they should report the incident immediately to a member of staff. Depending on the nature of the concern, it may be treated as a safeguarding issue under the Prevent strategy, ensuring that all learners are protected from the risks of radicalisation, exploitation and other forms of harm. This integrated approach ensures that Skills4 fulfils its duty of care to all learners, safeguarding their wellbeing and safety in both physical and digital environments.

VII. Staff conduct

Use of social media

Safeguarding learners is a key priority and, as such, the use of social media as a means by which members of staff communicate with learners requires clear guidance on appropriate use. Skills4 also has an Internet, Email and Social Media Usage Policy and Guidelines, which details the expectations of staff.

Communication with learners and colleagues

Communication between learners and colleagues, by whatever method, should take place within clear and explicit professional boundaries. This includes wider use of technology such as mobile phone text messaging, email, social media, video conferencing platforms such as Teams or Zoom, and messaging services.
Social media groups set up on behalf of Skills4, for example a departmental Facebook or other social media group, must have the prior consent of the Marketing Manager, who will keep a record of these groups and provide guidance on safe and professional use upon request. Groups will be subject to monitoring by the Marketing Department. All such groups must comply with the Safeguarding Policy and the Prevent and Radicalisation Policy.

Staff with learners as social media “friends”

The position at Skills4 is that staff should not befriend learners on social media because professional boundaries may be misconstrued. However, Skills4 recognises that some members of staff may have family members, partners, friends and/or professional connections who are learners who have studied at Skills4. These staff may therefore have a learner as a “friend” on their social network site and, as such, should inform their line manager so a record can be made. In these circumstances, staff should also take responsibility for ensuring that pictures and comments on social networks are not professionally damaging. Young apprentices with friends who are also learners at Skills4 should be aware of their conduct online now that they have the same professional responsibilities as other members of staff.

Cyberbullying

Cyberbullying is the use of Information and Communications Technology (ICT), particularly mobile phones, Teams, social media and the internet, to deliberately upset someone. It is recognised that staff, as well as learners, may become targets of cyberbullying. Like other forms of bullying, cyberbullying can seriously impact on the health, wellbeing and self-confidence of those targeted. Skills4 does not tolerate any kind of bullying, including cyberbullying, and incidents should be reported and will be taken seriously and addressed immediately.

Photographic images

It is recognised that there are times when photographic images of learners may enhance the learning experience or be required as evidence for coursework. Lessons may be recorded, and any use of images must be in accordance with UK GDPR and the Data Protection Act 2018.

VIII. Security

The safe use of technology is a key element in keeping learners safe, including appropriate measures to protect them from harmful online material. All staff must take reasonable steps to prevent inappropriate access to Skills4 systems, for example SharePoint.

All learners and staff at Skills4 have their own personal, password-protected Bud account for all learning and assessment activities.

All staff-issued laptops at Skills4 have security protection software installed to help prevent loss or corruption of data due to ransomware or virus attacks. All user network data is backed up to ensure that information can be restored when required.

All staff have access to the latest software to support effective and comfortable working, including any workstation requirements that individuals may have.

Skills4 is required under the DfE's statutory guidance, 'Keeping Children Safe in Education 2026', to keep learners safe online as well as offline. This includes limiting learners' exposure to potential risks and inappropriate or harmful content, ensuring that suitable filtering and monitoring arrangements are in place, and reviewing the effectiveness of these arrangements at least once every academic year. Any adverse incident affecting learners must be reported to line managers and to the DSL or DDSL in line with the Safeguarding Policy.

Filtering and monitoring arrangements must apply to Skills4-managed internet-connected devices and relevant learning environments, including remote and online delivery where applicable. Reviews should be led by the senior leader responsible for filtering and monitoring, with support from the DSL and IT support. Records should be kept of checks completed, issues identified, decisions made and actions taken.

Online safety expectations also include risks linked to new and emerging technologies, including artificial intelligence and AI-generated content. Staff must remain alert to the possibility that learners may access, create or be exposed to harmful, misleading, discriminatory, extremist, inappropriate or exploitative content online, and must report concerns through the established safeguarding routes.

Skills4 equipment, including laptops, should only be used for the purposes of the employed role, for example in workshops for teaching. This includes PCs and laptops used for exams and controlled assessments, to ensure exam regulations are followed. Computer usage during lessons must be course-related at all times.

Skills4 uses a perimeter firewall to protect the company's network services and devices. All activity data is kept securely and is only accessed on request by authorised members of staff, such as IT, safeguarding and management.

IX. Equality and Diversity

As with all Skills4 policies and procedures, due care has been taken to ensure that this policy is appropriate to all employees regardless of gender, race, ethnicity, disability, sexual orientation, marital status, gender identity, religion or age.

The policy will be applied fairly and consistently while upholding the organisation's commitment to providing equality for all.
If any employee feels that this or any other policy does not meet this aim, they should contact the HR Lead where necessary.

X. Version control

Version 1	28.08.2024	Policy creation
Version 2	07.08.2025	Policy annual update in line with Keeping Children Safe in Education 2025
Version 3	03.08.2026	Policy annual update in line with Keeping Children Safe in Education 2026