Online Safety Policy 2025/2026

Policy Author	Samantha Collins
Approved by	Jamie Crinigan
Position	Managing Director
Approved date	September 2025
Signed	
Next review date	August 2026
Version	2

1. 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 sufficient guidance to ensure that this commitment is embedded into the culture and ethos of the company. It is thus essential that all staff are aware of their duties regarding Online Safety and report any concerns promptly.

Designated Safeguarding Lead is referred to as DSL and Deputy Designated Safeguarding Lead is known as DDSL within this policy.

This policy has been agreed, sponsored, and approved by the Skills4 Board and Safeguarding Sub-Committee:

Name	Role
Jamie Crinigan	MD with overall accountability for Safeguarding and Prevent
Gail Crossman	Chair of Safeguarding Sub-Committee (SSC)
Sam Collins	Designated Safeguarding Lead (SSC member)
Victoria England	Deputy Designated Safeguarding Lead (SSC member)
Judi Oliver	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
Safeguarding & Inclusion Lead	Deputy Designated Safeguarding Lead (SSC member)

2. Purpose

This policy document outlines Skills4s approach to online safety in accordance with best practice in the FE Education sector. This policy has been written to provide guidance to staff regarding online or technological communications with learners or colleagues.

3. Introduction

This policy applies to all members of staff and learners who have access to Skills4s IT systems, including Microsoft Teams, both on the premises and remotely. The Online Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, video conferencing, social media and messaging services, online games, and any other systems that use the internet for communication and information storage. Additionally, this policy emphasises the importance of keeping learners safe both at home and at work online. It ensures that all users are aware of the potential risks associated with online activities and provides guidelines for safe and responsible use of digital tools and resources, aiming to protect the well-being of all users in any online environment.

4. 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 this responsible use. As part of our statutory duty to safeguard and promote 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 independently identify and manage risks.

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 student self-access, for example via Bud and SharePoint.
- Progress review meetings.
- Online teaching and learning sessions.

This Online Safety Policy outlines how best to use technology to 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 and also for those who are required to follow the GPhC standards for Pharmacy Professionals or General Dental Council standards.

The Online Safety policy should be read in conjunction with the Safeguarding Policy, the KCSIE 2025 requirements, the Internet, Email, and Social Media Usage Policy and Guidelines, the Prevent and Radicalisation Policy and Prevent risk assessment and action plan. Any member of staff found in breach of these policies and plans may be subject to disciplinary processes, ensuring compliance with our broader safeguarding duties, including those associated with the Prevent strategy.

5. 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 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 evidenced based research purposes, avoiding any misinformation.
- Develop skills to evaluate information on the internet.
- 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 as per 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 concerns about 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 students.
- 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 ensure data is safe and secure and access to unsuitable content is disabled 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 members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.
- Should model safe, responsible, and professional behaviours in their own use of technology at Skills4Pharmacy and in their personal use.
- Ensure compliance with associated policies and risk assessments e.g. Safeguarding Policy, Prevent Radicalisation Policy and Prevent risk assessment and action plan.

6. 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 institution. 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 Skills4Pharmacy community.
- Are contrary to Equality, Diversity, and Inclusion.
- Explicitly encourage others to break the law.

- Are likely to bring Skills4Pharmacy into disrepute.

These guidelines are critical not only for maintaining a respectful and professional learning environment but also for aligning with Skills4 commitment to both 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 counter 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 cause for 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 the physical and digital environments.

7. Staff conduct

Use of Social Media

Safeguarding students is a key priority and, as such, the use of social media as a means by which members of staff communicate with students 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 Students and Colleagues

Communication between learners and colleagues, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as

mobile phone text messaging, emails, social media, video conferencing 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 be with 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 Prevent and Radicalisation Policy.

Staff with Students as social media "friends"

The position at Skills4 is that staff should not befriend students on social media because professional boundaries may be misconstrued. However, Skills4 recognises that some members of staff may have family members, partners and/or friends, and professional connections who are learners who have studied at Skills4. These staff may therefore have a student 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 students 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 students, may become targets of cyberbullying. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. Skillls4 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 necessary evidence for coursework. Lessons will be recorded and so any imaging must be in accordance with UK GDPR and the Data Protection Act 2018.

8. Security

The safe use of technology is a key element to keep learners safe including appropriate measures to protect them from harmful online materials. All staff must take reasonable measures 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 use for all learning and assessment activities.

All staff issued laptops at Skills4 have security protection software on them to help prevent loss or corruption of data due to ransomware and virus attacks. All user network data is backed up to ensure we can restore information as and when requested.

All staff have access to all the latest software to allow them to work easily and comfortably meeting workstation requirements that individuals may have.

Skills4 is required under the DfE's statutory guidance, 'Keeping Children Safe in Education' to keep students safe online. This includes ensuring that there is limited exposure to potential risks and inappropriate or harmful content. Any adverse incidents effecting learners must be reported to line managers.

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

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

9. 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 whilst upholding the organisation's commitment to providing equality to all.

If any employee feels that this or any other policy does not meet this aim, please contact the HR Lead if necessary.

10. Version control

Version 1	28.08.2024	Policy creation
Version 2	07.08.2024	Policy annual update