Online Safety and Social Media Policy

Item	Details
Policy owner	Matt Malkin
Position	Managing Director
Version	Version 2
Applies to	Learners and Staff
Effective from	August 2026
Review date	August 2027

1. Policy Statement

Skills-UK, Education & Training Limited is committed to promoting the safe, responsible and professional use of digital technology, online communication and social media.

Technology supports teaching, learning, assessment and communication. Skills-UK recognises that its use can also expose learners and staff to safeguarding concerns, abuse, fraud, inappropriate content and risks to privacy and information security.

Skills-UK will use appropriate safeguards, staff training, learner guidance and clear reporting arrangements to reduce these risks.

Online safety is part of Skills-UK's wider safeguarding responsibilities and applies to activity taking place at community venues, remotely and through digital communication.

2. Purpose and Scope

This policy sets out expectations for:

- safe and responsible use of digital technology;
- communication between staff and learners;
- professional boundaries online;
- use of social media;
- protection of personal and confidential information;
- recognition and reporting of online concerns; and
- responding to online safety incidents.

It applies to employees, associates, contractors and learners using Skills-UK systems or participating in Skills-UK activity.

It covers Skills-UK equipment and accounts, authorised use of personal devices, online learning platforms, email, telephone calls, text messages, WhatsApp, social media and other approved digital services.

It also applies to conduct outside normal working or learning hours where that conduct affects safeguarding, professional responsibilities or the safety of the Skills-UK community.

3. Responsibilities

Directors and Senior Managers

Directors and senior managers are responsible for ensuring appropriate online safety arrangements are in place, resources are available and significant concerns are addressed.

Policy Owner

Matt Malkin is responsible for coordinating the review of this policy and ensuring that relevant changes to working practices, technology and guidance are considered.

Designated Safeguarding Lead and Safeguarding Team

The safeguarding team is responsible for:

- receiving and responding to online safeguarding concerns;
- assessing risks and arranging appropriate support;
- making referrals where required;
- maintaining secure safeguarding records; and
- identifying learning from incidents.

Staff

All staff must:

- maintain professional boundaries in digital communication;
- use approved accounts, numbers, systems and services;
- provide appropriate online safety guidance to learners;
- protect personal and confidential information;
- report safeguarding and security concerns promptly; and
- follow this policy and associated Skills-UK procedures.

Staff must not promise absolute confidentiality when a safeguarding concern is disclosed. Information must be shared only with those who need it to protect individuals or respond appropriately.

Learners

Learners are expected to:

- communicate respectfully;
- use technology safely and responsibly;
- protect their passwords and personal information;
- follow instructions for Skills-UK equipment and learning platforms; and
- tell a member of staff if something online makes them feel unsafe, worried or uncomfortable.

Staff Responsible for IT Systems and External IT Support

Those responsible for IT systems must maintain appropriate technical safeguards, manage access, respond to security incidents and promptly refer safeguarding concerns to the safeguarding team.

4. Online Risks and Learner Education

Online safety guidance will be appropriate to learners' ages, needs, experience and programmes.

Guidance should help learners recognise and respond to:

- bullying, harassment, discrimination and threatening behaviour;
- grooming, sexual exploitation and coercive relationships;
- requests for intimate images and threats to distribute them;
- harmful or illegal content;
- radicalisation and terrorist content;
- scams, impersonation, phishing and financial exploitation;
- misleading information, manipulated images and deepfakes;
- unsafe sharing of personal information or location details; and
- harmful online interactions, including those involving gaming, livestreaming and social media.

Learners should understand that online identities and content may be false or misleading. They should be encouraged to check information, question requests and seek support without fear of blame.

Online safety will be addressed through induction, teaching and learning, relevant discussions and additional guidance where concerns arise.

5. Approved Communication with Learners

Skills-UK permits staff to communicate with learners through:

- Skills-UK email;
- telephone calls;
- text messages; and
- WhatsApp.

Other platforms may be used where authorised by Skills-UK.

Staff must use Skills-UK-provided or expressly authorised work accounts and telephone numbers. Approval of WhatsApp does not automatically authorise the use of an employee's personal account or number.

Communication must relate to legitimate Skills-UK activity, such as enquiries, enrolment, attendance, learning, assessment, appointments and learner support.

Messages and calls must be professional, respectful and appropriate to the learner's needs.

Staff must:

- check contact details before sending information;
- consider whether the channel is suitable for the information involved;
- avoid unnecessary personal or sensitive details;
- respect reasonable contact preferences and accessibility needs; and
- transfer significant information into the appropriate Skills-UK record.

Staff are not expected to provide continuous availability or respond outside their agreed working arrangements.

Learners must be informed that messages may not be read immediately and that email, text messages and WhatsApp are not emergency services.

6. WhatsApp and Group Messaging

WhatsApp may be used for legitimate Skills-UK communication where appropriate safeguards are followed.

Staff must:

- use an authorised work account or number;
- secure the device with an appropriate screen lock;
- enable available account security measures;
- prevent unauthorised access to messages;
- avoid personal cloud backups or linked devices unless authorised;
- check recipients before sending messages or attachments; and
- retain necessary organisational records in approved systems.

WhatsApp must not become the sole record of safeguarding concerns, assessment decisions, complaints or other significant matters.

Sensitive information should be moved to a more appropriate approved system where necessary. Staff must not ask learners to share sensitive documents through WhatsApp simply for convenience.

Before creating a group, staff must consider its purpose, membership, moderation and the personal information visible to participants.

Learners must be told if joining a group will disclose their telephone number, profile information or other details to others. An appropriate alternative must be available where a learner does not wish to participate.

Groups must have clear expectations for conduct. Staff must promptly address inappropriate content and remove access when it is no longer required.

Disappearing messages must not be used where they would prevent Skills-UK from meeting safeguarding, recordkeeping or other organisational requirements.

7. Professional Boundaries and Personal Social Media

Staff must maintain professional boundaries with learners across all digital services.

Staff must not:

- use learner contact details for personal purposes;
- initiate or encourage private social relationships through learner communication;
- send sexual, suggestive, intimidating or otherwise inappropriate messages;
- request personal images unrelated to an authorised learning purpose;
- move conversations to private or secret channels; or
- use digital communication to exploit a position of trust.

Staff must not initiate or accept personal social media connections with current learners. Professional contact through an authorised organisational account may be appropriate.

Any pre-existing family, friendship, community or other connection that could affect professional boundaries must be declared to a manager or safeguarding lead so that suitable arrangements can be agreed.

Boundaries must continue to be considered after a learner leaves, particularly where the person is under 18, is an adult at risk or remains dependent on staff support.

Staff must not assume that a relationship becomes appropriate simply because a learner has completed their programme.

Personal social media activity must not disclose confidential information, identify safeguarding cases or suggest that personal opinions are official Skills-UK statements.

8. Official Social Media Accounts

Only authorised staff may create, access or publish through accounts representing Skills-UK.

Skills-UK must retain organisational control of official accounts, including recovery arrangements and appropriate administrator access.

Content must:

- be accurate, respectful and appropriate;
- follow Skills-UK branding and communication expectations;
- protect personal and confidential information;
- respect copyright and licensing requirements; and
- use learner images and stories only where appropriately authorised.

Account access must be reviewed when staff responsibilities change or employment ends.

Inappropriate comments, impersonation, account compromise and safeguarding concerns must be reported promptly.

Statements about serious incidents, emergencies or safeguarding matters must be approved by a Director or their nominated representative before publication.

9. Acceptable Use and Cyber Security

Staff and learners must use Skills-UK systems lawfully and responsibly.

They must not:

- access accounts or information without permission;
- share passwords or use another person's identity;
- deliberately introduce harmful software;
- bypass security controls without authorisation;
- bully, harass, threaten or exploit others;
- access or distribute illegal material; or
- upload confidential information to unauthorised services.

Devices and accounts must be protected through appropriate passwords, access controls, updates and multifactor authentication where available and required.

Suspicious links, attachments, payment requests and requests for login information must be treated cautiously. Unusual requests should be checked through a known and trusted contact route.

Lost devices, compromised accounts, suspicious messages and accidental disclosures must be reported promptly.

10. Community Venues and Personal Devices

Skills-UK delivers from community, partner and other third-party venues and may not control their internet connections or technical safeguards.

Before internet access is used for delivery, staff must consider the venue arrangements, the planned activity and any additional controls needed.

Staff must not assume that venue Wi-Fi provides filtering, monitoring or protection equivalent to Skills-UK-managed systems.

Appropriate precautions may include supervised use, checking online resources in advance, using approved connections and restricting activities involving sensitive information.

Personal devices may be used for learning where appropriate. Learners must follow session expectations and must not photograph, record or share information about others without appropriate permission.

Staff use of personal devices for Skills-UK work requires authorisation and suitable security arrangements. Personal or household users must not be able to access Skills-UK information.

11. Online Teaching and Meetings

Staff must use approved platforms and apply appropriate access and privacy settings.

They should:

- check participants and control access where appropriate;
- avoid publishing meeting links openly unless intended;
- explain expected behaviour;
- consider accessibility and support needs;
- use professional surroundings and presentation; and
- respond promptly to inappropriate participation or content.

One-to-one online sessions must have a legitimate purpose and follow appropriate safeguarding arrangements.

Sessions must not be recorded routinely. Any recording requires an identified purpose, appropriate authorisation, a lawful basis, advance information for participants and secure retention arrangements.

12. Monitoring and Filtering

Skills-UK will determine appropriate filtering, monitoring and access controls through consideration of its systems, learners, activities and safeguarding risks.

Technical controls will support staff supervision and learner education. They cannot prevent every harmful interaction or identify every concern.

Skills-UK will clearly explain any monitoring it undertakes, including its purpose, scope, access arrangements and retention of information.

Monitoring must be necessary, proportionate and consistent with applicable data protection requirements. Access to monitoring information must be restricted to authorised individuals.

Skills-UK will not claim to monitor all communications or personal internet activity where it does not have that capability.

13. Safeguarding and Prevent

Online safeguarding concerns must be reported promptly through Skills-UK's safeguarding arrangements.

This includes concerns about exploitation, abuse, coercion, sexual harassment, intimate-image abuse, self-harm, radicalisation and threats of violence.

Staff must support respectful discussion and distinguish lawful expression, disagreement or controversial views from behaviour that indicates harm or a safeguarding risk.

Staff should challenge discriminatory, abusive or threatening behaviour appropriately. They must not attempt to investigate suspected radicalisation or confront individuals in a way that increases risk.

Decisions about safeguarding support and external referrals must follow the relevant Skills-UK procedures.

Concerns about a member of staff must follow the procedure for allegations or concerns about staff conduct, including an alternative reporting route where the usual recipient is implicated.

14. Reporting and Responding to Incidents

Anyone experiencing or witnessing an online concern should tell a member of staff or contact the safeguarding team.

Staff receiving a concern must:

- listen calmly and take it seriously;
- consider immediate safety and support needs;
- explain that relevant information may need to be shared;
- record factual information securely; and
- report promptly through the appropriate safeguarding, management or IT route.

Call 999 where there is immediate danger or an emergency requiring police, ambulance or fire services.

Staff must not undertake their own investigation, contact a suspected offender or promise a particular outcome.

Evidence should be handled safely. Where appropriate, record details such as usernames, dates, times and the location of content without unnecessarily copying or circulating harmful material.

Where sexual images of a person under 18 may be involved, staff must not deliberately view, copy, download, print, forward or save the images, or ask anyone to send them. The matter must be referred immediately to the safeguarding lead for action under the relevant guidance.

Suspected personal data breaches must also be reported immediately to the person responsible for data protection so that reporting obligations can be assessed within the applicable timescales.

The responsible lead will coordinate support, referrals, technical action, recordkeeping and follow-up.

15. Personal Information and Images

Personal information must be processed in accordance with applicable UK data protection legislation and Skills-UK's privacy and data protection arrangements.

Staff must use only the information necessary for the task and share it only with authorised recipients through suitable channels.

Photographs, videos, recordings and learner stories require an appropriate lawful basis and clear information about their intended use.

Where consent is relied upon, it must be appropriately obtained and recorded. Learners must not be pressured to agree to promotional use.

Images and recordings must be stored securely in approved systems and retained only for as long as necessary.

Staff and learners must not publish images that expose private information, reveal safeguarding concerns or place an individual at risk.

16. Artificial Intelligence and Copyright

AI tools may be used only in accordance with Skills-UK's approved arrangements and any relevant awarding organisation requirements.

Staff and learners must not enter identifiable learner information, safeguarding records, confidential documents or other restricted information into unapproved AI services.

AI-generated content must be checked for accuracy, bias, suitability and misleading information. It must not replace professional safeguarding judgement.

AI must not be used to impersonate others, create abusive or sexualised content, manipulate evidence or misrepresent assessment work.

Staff and learners must respect copyright, licences and permitted educational uses. Acknowledging a source does not, by itself, authorise copying or publication.

17. Recruitment and Online Checks

Any online checks used during recruitment must be relevant, proportionate, transparent and consistent with Skills-UK's safer recruitment and data protection arrangements.

Applicants must be informed where such checks form part of the recruitment process.

Information unrelated to suitability for the role must not influence selection decisions. Staff must not seek access to private accounts or use deceptive methods to obtain information.

Potential concerns must be considered fairly and through the appropriate recruitment process.

18. Training and Policy Review

Staff will receive relevant online safety guidance during induction and updates appropriate to their roles.

Training should cover professional boundaries, approved communication, safeguarding reporting, information security and emerging online risks.

Breaches of this policy will be considered under the relevant staff, learner or contractual procedures. Responses will reflect the circumstances, seriousness, support needs and safeguarding implications.

This policy will be reviewed at least annually and sooner where significant incidents, changes in technology, working practices or relevant requirements make this necessary.

It should be read alongside Skills-UK's safeguarding, Prevent, acceptable use, data protection, staff conduct, learner behaviour, anti-bullying, complaints and disciplinary arrangements.