E-Safety and Social Media Policy - Staying Safe Online

Applicability

This policy/procedure/process applies to all divisions, subsidiaries, departments, and associated organisations within Twin Group. It is binding on all employees, contractors, and stakeholders engaged in activities on behalf of the Group, regardless of business unit or location. All members of the Group are expected to adhere to the principles, standards, and requirements set out herein.

Introduction

We recognise that online learning and digital technologies provide incredible opportunities for participants and learners to learn, collaborate, and develop new skills. However, using these technologies safely requires clear guidance for everyone involved, learners, teaching & delivery staff, and employers.

This guidance sets out expectations, responsibilities, and best practices to ensure that all online learning is safe, professional, and effective. It applies to live and pre-recorded learning sessions, as well as any learning materials shared digitally.

Purpose

The purpose of this guidance is to:

- Ensure that all participants, learners, teaching & delivery staff, stakeholders, and employers understand their responsibilities when engaging in online learning.
- Provide a safe and respectful online environment for learning.
- Protect personal data, privacy, and professional boundaries.
- Support consistent standards in delivery, safeguarding, and professional conduct across all platforms and settings.
- Give employers and partners clear expectations for engagement and conduct in any online learning provision.

Scope

This policy applies to:

- All teaching & delivery staff delivering online or in-person learning.
- Learners and participants accessing learning through digital or online platforms.
- Employers and stakeholders attending or supporting online learning sessions.
- All platforms used for learning, collaboration, and communication.
- All subcontractors involved in the delivery of learning or learner support activities.

We ensure that as part of safeguarding responsibilities, the following are in place:

- Clear policies and acceptable use guidance that are reviewed and updated regularly.
- Training and supervision for staff.
- Education for learners on safe digital use.
- Procedures for reporting misuse or abuse of technology.

Contents

1. General Considerations

All participants, learners, teaching & delivery staff, and employers should:

- Understand that safeguarding policies fully apply in digital environments, including online learning platforms, social media, and collaborative tools.
- Immediately report any concerns or incidents to their manager, the designated safeguarding lead, or the IT Department.
- Respect copyright, licensing, and data protection laws when creating, sharing, or using materials online.
- Maintain accurate records of online sessions (including 1:1 sessions), including attendance, duration, and any technical issues, to ensure transparency and evidence of learning activity.
- Promote safe and respectful behaviour during online interactions, including discussions, video calls, forums, and collaborative platforms.
- Learners and participants must understand and follow the Code of Conduct, (as described at induction), which outlines expected behaviour, responsibilities, and safe use of digital tools.

2. Use of Internet, Mobile, and Digital Technologies

All users are expected to use digital technologies responsibly and ethically. Users must not:

- Access, post, share, or distribute indecent, discriminatory, illegal, or offensive material.
- Upload or distribute copyrighted content without permission.
- Disclose confidential or personal information about others.
- Disrupt online systems or introduce malware, viruses, or other security threats.
- Use mobile or digital technologies to intimidate, threaten, bully, or harm others.

Employers supporting learners should:

- Encourage safe online participation for learners under their supervision.
- Respect privacy and professional boundaries.
- Report concerns promptly if issues arise during online sessions.
- Reinforce learners' understanding of safe online practices and adherence to the Code of Conduct.

Learners and participants should:

- Follow the Code of Conduct in all online interactions.
- Report unsafe or inappropriate online behaviour immediately.
- Understand that failure to comply with the Code of Conduct may lead to restricted access or disciplinary action.

Subcontracted Partners supporting learners should:

- Not post or permit to be posted any material that breaches confidentiality, data protection, intellectual property, or contractual obligations to Twin Group or its clients.
- Not use Twin Group's brand, logo, client names, or identify themselves as acting on behalf of Twin Group unless expressly authorised in writing.
- Not engage in online conduct likely to bring Twin Group or its clients into disrepute, including harassment, discrimination, defamation, bullying, or unlawful content.

- When posting via personal accounts where they are identifiable with Twin Group, clearly state that views are personal and do not represent Twin Group (e.g. “These are my own views and not those of Twin Group”) unless otherwise authorised.
- Comply with Twin Group’s policies on data protection, confidentiality, branding, and communications when producing social media content or engaging in online communications.
- Ensure that all devices, networks, and online platforms used in delivering Twin Group contracts are secure (including the use of strong passwords, encryption where applicable, and up-to-date security software).
- Not upload or share Twin Group or client data via social media platforms, messaging apps, or public forums unless expressly authorised and done so under secure and controlled protocols.
- Immediately (or within 24 hours) report any social media or online incidents, such as data breaches, sharing of sensitive content, inappropriate posts, cyberattacks, or phishing attempts to the Quality & Standards Manager, who will escalate the matter to Twin Group’s Information Security Officer.

3. Reporting Concerns or Abuse

- Any incidents involving unsafe online activity, abusive content, or accidental access to harmful material must be reported immediately to the IT Department and Designated safeguarding lead.
- Safeguarding procedures will be followed to protect learners and participants.
- Subcontracted partners must follow the same reporting process as Twin Group staff and ensure any incidents are reported to both their own Designated Safeguarding Lead (where applicable) and Twin Group’s DSL within 24 hours of becoming aware of the concern.
- Subcontractors must not investigate incidents independently but should record factual information and escalate promptly to ensure Twin Group can manage the concern in line with its safeguarding and information-security policies.
- Disciplinary processes may be initiated where appropriate for staff, learners, or participants.

4. Infrastructure, Technology, and Partnership Working

- All online platforms, digital resources, and technology infrastructure are maintained to ensure secure, monitored, and compliant use.
- Employers, stakeholders, and external organisations participating in online learning are expected to have appropriate e-safety policies and safeguarding procedures.
- All digital content and resources must be accessible, inclusive, and suitable for learners with diverse needs.
- Subcontracted partners delivering or supporting online learning on behalf of Twin Group must use approved systems and platforms that meet Twin Group’s data protection, security, and accessibility standards.
- Subcontractors must ensure their own infrastructure, devices, and networks are secure, using up-to-date software, encrypted data storage (where applicable), and controlled access for authorised personnel only.

- Any digital platforms or tools introduced by subcontractors must be approved in advance by Twin Group's IT to ensure compatibility, learner safety, and compliance with safeguarding and information security protocols.
- Twin Group will maintain oversight of all subcontracted delivery to ensure systems, safeguarding arrangements, and learner experiences meet organisational and contractual standards.

5. Social Media use

Personal Use

Teaching & delivery staff must:

- Not engage in private communications with learners, participants, or stakeholders on personal social media platforms.
- Report any inappropriate, concerning, or unsafe communications immediately to the IT Department.
- Ensure all personal social media accounts have the highest privacy settings and avoid sharing personal opinions, photos, or content that could damage the organisation's reputation or undermine trust.
- Use official email accounts for all communications related to learners, participants, or online learning activities. Personal emails, mobile numbers, or messaging apps should not be used for professional contact.

Learners and participants should:

- Avoid sharing personal contact details with staff or employers on social media.
- Report any concerning messages or inappropriate contact from peers, staff, or external parties.
- Be mindful of their digital footprint and avoid posting material that could harm their own reputation or that of the organisation.

Employers and stakeholders supporting learning:

- Must maintain professional boundaries and avoid connecting with learners or participants on personal social media accounts.
- Report any concerning interactions observed during online sessions.

Subcontracted Partners Supporting Learning:

- Must not engage in private social media communications with learners or Twin Group staff.
- Ensure all personal and professional accounts are used appropriately, maintaining confidentiality, professionalism, and compliance with Twin Group's Code of Conduct.
- Not post or permit posting of any content that breaches data protection, confidentiality, intellectual property, or contractual obligations to Twin Group or its clients.
- When identifiable as affiliated with Twin Group, clearly state: "These are my own views and not those of Twin Group" unless expressly authorised otherwise.
- Comply with Twin Group's branding, communications, and data security policies when referencing work, projects, or learners online.
- Immediately report any inappropriate or concerning online content, breaches, or reputational risks to the Quality & Standards Manager.

Professional / Sanctioned Use

Social media may be used to enhance learning and engagement through professional, sanctioned accounts. All users must follow these principles:

Teaching & delivery staff:

- Create distinct professional social media accounts for educational purposes, separate from personal accounts, and ideally linked to official organisational emails.
- Ensure content is professional, accurate, and appropriate, reflecting positively on the organisation.
- Obtain explicit written consent from learners, participants, parents/guardians, or stakeholders before posting photographs, videos, or personally identifying information.
- Regularly monitor the accounts for inappropriate content, comments, or interactions, and report or remove anything that breaches policy.
- Provide guidance to learners on safe online engagement, encouraging respectful communication, responsible sharing, and digital literacy.
- Include a visible link to the organisation's E-Safety policy on all sanctioned social media accounts, so users are aware of expected behaviours.

Learners and participants:

- Use professional social media accounts or learning platforms only for educational purposes.
- Do not share passwords or login details with peers.
- Avoid posting personal information that could identify themselves or others without permission.
- Follow staff guidance on acceptable online behaviours and report any unsafe or inappropriate content immediately.

Employers and stakeholders:

- Only use professional, sanctioned social media accounts when supporting learning activities.
- Respect privacy, maintain professional boundaries, and avoid sharing learner information without consent.
- Reinforce safe online practices for learners and participants under their supervision.

Subcontracted Partners Supporting Learning:

- Only use Twin Group–approved or sanctioned accounts when promoting, delivering, or supporting learning activities.
- Seek written authorisation before posting any learner, programme, or partnership-related content referencing Twin Group.
- Monitor professional accounts for compliance and remove or report any content that breaches Twin Group standards.
- Ensure all online engagement supports Twin Group's values of inclusion, professionalism, and learner safety.

General Guidance for Safe Social Media Use

- Never post content that is discriminatory, offensive, or illegal.
- Avoid engaging in debates or arguments that could escalate publicly on social media platforms.
- Protect personal and organisational reputations by thinking carefully before posting or sharing content.
- Report suspected online bullying, harassment, or inappropriate behaviour immediately.
- Understand that all digital communications may be recorded or monitored and can be used as evidence in safeguarding investigations.
- Subcontracted partners must follow these same principles and ensure that any representatives or delivery staff working under their contract do so as well. Non-compliance may result in contract review or termination.

6. Inclusion and Accessible Digital Learning

We are committed to ensuring that all learners, participants, teaching & delivery staff, and employers have equitable access to online learning opportunities.

Key principles include:

- Accessibility: Digital content must be accessible to all, with alternative formats as needed.
- Equal Participation: All learners should fully engage in online learning, discussions, and collaborative activities without discrimination.
- Support for Diverse Needs: Staff and employers should actively identify and remove barriers to participation.
- Safe and Respectful Environment: Digital spaces must promote respect and inclusion for all.
- Employer Engagement: Employers participating in learning must ensure inclusivity and encourage safe, equitable participation.
- Subcontracted Partners: Must ensure all online delivery and learning materials meet accessibility standards, promote equality, and reflect Twin Group's inclusion and safeguarding values.

7. Monitoring, Standards, and Sanctions

Online platforms, mobile technology, and social media use are regularly monitored for safety and compliance.

Breaches may result in the following:

Learners / Participants:

- Restrictions on digital access or disciplinary action.
- Serious incidents may be referred to relevant authorities.

Teaching & Delivery Staff:

- Disciplinary action for breaches.
- Serious incidents may be referred to authorities.

Employers / Stakeholders:

- Serious incidents may be referred to authorities.
- Immediate reporting of inappropriate material is required to the IT Department or safeguarding lead.

Subcontracted Partners:

- Breaches of this policy may lead to formal investigation, suspension of delivery, or termination of contract.
- Failure to comply with reporting or data security requirements will be treated as a breach of contractual and safeguarding obligations.
- Subcontractors must cooperate fully with any Twin Group investigations or audits arising from online safety or social media incidents.