Online Safety Policy

Online Safety & Artificial Intelligence (AI) Usage Policy

Riverside Training is committed to ensuring that all staff and learners are safe and responsible in their use of digital technologies. This includes internet access, social media, mobile devices, and newer technologies such as Artificial Intelligence (AI). As a modern training provider, we aim to embrace the benefits of these tools while safeguarding individuals and maintaining professional standards.

This policy sets out our expectations for safe, ethical, and lawful use of online tools and AI technologies, and outlines the procedures for reporting and managing any concerns.

Purpose and Scope

The purpose of this policy is to ensure that all users, including staff, Learner Development Coaches (LDCs), contractors, and learners, understand how to use technology safely and appropriately. It covers internet use, social media activity, the use of digital devices, and any interactions involving AI technologies, whether for communication, learning, or administration.

The policy aims to protect users, uphold data protection and safeguarding responsibilities, and maintain a professional digital environment across all platforms associated with Riverside Training.

Online Safety and Use of Technology

All individuals involved with Riverside Training are expected to use technology respectfully and with care. The same standards of safety and professional conduct apply regardless of the device used – whether it is a computer, mobile phone, tablet, or smart device.

Staff and learners must use the internet, websites, email, and social media responsibly. Access to digital platforms must never be used to bully, harass, or abuse others. Disclosures of any form of online abuse, including cyberbullying or inappropriate messages, will be taken seriously and managed in line with our safeguarding procedures.

Smartphone users are reminded to respect the privacy of others. Images or videos must not be taken or shared without consent. Sexting, or the sharing of explicit or offensive material, is strictly prohibited.

All digital behaviour must reflect the values and professionalism of Riverside Training.

Social Media and Public Platforms

Riverside Training maintains a professional online presence via its website and social media channels. These platforms are monitored and managed by an authorised member of staff. Content posted to these channels must reflect the organisation's values and be appropriate for public and professional audiences.

All official accounts are password protected. A designated person will oversee activity and liaise with the safeguarding lead where appropriate. Inappropriate posts will be removed, and concerns investigated.

Staff must not communicate with learners using their personal social media accounts. Professional boundaries must be maintained at all times. This includes avoiding the use of informal language, emojis, or symbols such as 'kisses' (X's) in communication with learners. Email and messaging accounts should be used only through official Riverside Training systems.

Artificial Intelligence (AI) Usage

Riverside Training supports the careful and responsible use of AI technologies to assist with learning, planning, and administrative tasks. AI tools may be used to generate ideas, summarise content, check spelling or grammar, or support the creation of learning materials – but always under human oversight.

AI must be used to support, not replace, critical thinking, creativity, and learner development. For staff, AI can offer efficiencies, but must not be relied upon without review. For learners, AI may be used as a tool to aid understanding or generate ideas – but assessments and evidence of learning must always be the learner's own work.

Using AI to complete work on behalf of someone else, especially in relation to assessments, is a form of academic dishonesty and will be dealt with accordingly.

Data Protection and Security

All use of digital and AI tools must comply with the UK General Data Protection Regulation (UK GDPR). Staff and learners must not enter personal, identifiable, or sensitive information into public AI tools unless they are approved by Riverside Training and confirmed to meet data protection standards.

Riverside Training will ensure that any digital tools or platforms used for communication, learning, or content creation are secure, appropriate, and suitable for educational use. Staff are responsible for ensuring data is handled correctly and that no personal data is shared or processed in ways that could put individuals at risk.

Responsibilities of Staff and Learners

All staff, including LDCs, are responsible for promoting safe and professional digital behaviour. Staff must role-model appropriate use of technology, support learners in developing safe digital habits, and report any breaches of this policy.

Learners are expected to engage responsibly with online tools, platforms, and resources. They must never attempt to deceive or misrepresent work through the use of AI or digital manipulation.

Any disclosures of abuse made online, including via social media or AI platforms, must be treated with the same seriousness as face-to-face disclosures. They must be reported promptly to the safeguarding team and managed in accordance with the organisation's safeguarding policy.

Breaches of Policy

Any breach of this policy, by staff or learners, may result in disciplinary action. For staff, this could include formal warnings or dismissal. For learners, this could result in removal from a programme or withdrawal of access to training resources.

Inappropriate digital behaviour, misuse of AI, unauthorised sharing of content, or failure to maintain professional conduct online will not be tolerated.

Monitoring and Reporting

All digital activity related to Riverside Training systems may be monitored to ensure compliance with this policy. Staff should report any concerns about digital safety, inappropriate content, or AI misuse to their line manager or the safeguarding lead as soon as possible.

Safeguarding concerns raised through digital platforms must be recorded and acted upon in line with existing safeguarding protocols.

Monitoring & Review

This policy is reviewed annually

Current Review Date	July 2026
Next Review Date	July 2027

Online Safety Policy