

Social Media Policy



Riding Establishment:

Overview

This policy outlines the responsibilities of employees, volunteers, and contractors when using social media, whether personally or on our behalf. It applies to all use of social media on our premises, during working hours or in connection with our activities. Use of our IT systems may be monitored to ensure compliance, and by accessing these systems, individuals consent to such monitoring.

Breaches of this policy may result in disciplinary action under our Disciplinary Policy and Procedure. Individuals may be required to remove content that violates this policy, and failure to do so may lead to further action. Legal proceedings may also arise if posts harm our reputation or named individuals.

Definition of Social Media

Social media refers to websites and applications that enable users to create, share, and engage with content or networks. This includes platforms such as Facebook, Twitter/X, LinkedIn, Instagram, TikTok, YouTube, Reddit, and others, as well as blogs, forums, and online noticeboards.

Accessing and Using our Social Media Accounts

Only authorised individuals may access and post to our official social media accounts. Personal accounts must not be used for organisational purposes. Privacy settings must remain as configured by us, and any concerns about settings should be raised with a manager. Access should be via approved devices only, unless explicit permission has been granted.

Safeguarding and Digital Conduct

Individuals must be mindful of their digital footprint. Children, young people, adults at risk, and their families may view social media accounts linked to us. Posts must be age-appropriate, respectful and free from harmful or discriminatory content. Personal contact details must not be shared, and friend requests or private communications with clients or their families via personal accounts are strictly prohibited.

Images and videos may only be shared on our accounts with prior written consent. Where consent is not granted, identifying features must be obscured. All media must reflect positively on the individual's involvement and uphold safeguarding principles.

Personal Social Media Use

Personal use of social media during working hours is not permitted unless explicitly required for the role. Our social media accounts must not be used for personal content. Upon leaving us, access to accounts will be revoked, and individuals must provide any relevant usernames and passwords.

When using personal accounts, individuals must clearly state that views expressed are their own and not those of the organisation. Personal email addresses should be used, and care must be taken to avoid creating accounts that could be mistaken for official channels. Individuals must not post content that could damage our reputation or breach confidentiality.

Respectful and Lawful Communication

All social media use must be respectful and lawful. Individuals must not criticise us, clients, colleagues, contractors or partners. Behaviour that would be unacceptable in the workplace, such as harassment, bullying, or discriminatory language, is equally unacceptable online. Specifically, the following are prohibited:

- Abusive or threatening language
- Sexually explicit or unlawful content
- False or misleading statements
- Impersonation or incitement to commit a crime

Grievances must not be aired on social media. Concerns should be raised internally with a line manager and, if unresolved, through the formal grievance procedure.

Confidentiality and Intellectual Property

Confidential information must never be shared on social media. This includes trade secrets, internal communications and any material not in the public domain. Our logo, branding, and artwork must not be used without permission.

Social media is inherently public. Even restricted posts can be shared widely, and individuals must assume that anything published may reach the public domain. Sharing others' content may imply endorsement, so discretion is advised.

Copyright and Contact Data

Copyright must be respected. Before reposting third-party content, individuals must confirm that it is not protected or that permission has been granted. Business contact details acquired during employment or volunteering remain the property of the organisation and must be returned and deleted upon departure.

Breach of Policy

Any suspected breach must be reported to a line manager immediately. Disciplinary action may be taken regardless of whether the breach occurred during working hours or using our equipment. Individuals may be required to cooperate with investigations, including providing login credentials. Refusal to remove offending content may result in further action.