STAFFPOWER GROUP

RECRUITMENT & TRAINING

Social Media Policy

| Version 2.0 |

Policy Commencement Date	20/08/2026
Policy Version	2.0
Review by	20/8/2027
Document Controller	Jonathan Hall
Signature	*J.Hall*

Contents page

Content	Page
1. Introduction	2
2. Scope	2
3. Roles and Responsibilities	2
4. Key Legislation and Guidance	3
5. Key Principles of the Online Safety Policy	4
6. Official Social Media Use	4
7. Social Media Content Standards	4
8. Personal Social Media Use	5
9. Reputational Risk and Professional Conduct	6
10. Safeguarding and Online Safety	6
11. Data Protection (GDPR)	8
12. Reporting a Concern	8
13. Breaches of Policy	8
14. Further Guidance	9
15. Policy Review	9

2.0 Policy Update Summary

This policy has been comprehensively reviewed and updated to strengthen governance, safeguarding, online safety, data protection, and reputational risk management arrangements across Staff Power Training. The revised version provides clearer guidance on the appropriate use of social media, expands the scope of the policy, and introduces defined roles and responsibilities for leaders, staff, learners, and account administrators.

Key enhancements include the introduction of detailed social media content standards, strengthened safeguarding and reporting procedures, clearer expectations regarding professional conduct and reputational risk, and improved alignment with current legislation and best practice guidance. The policy now also makes explicit links to related organisational policies and provides a more robust framework for managing social media activity and associated risks.

1. Introduction

1.1 This policy outlines the procedures and guidance for ensuring the online safety of all learners and staff at Staff Power Training (SPT). Our aim is to create a safe and respectful online environment that allows for effective learning while protecting individuals from potential harm. It has been developed in line with key national guidance, including the UK government's "Keeping Children Safe in Education" and best practice recommendations from the UK Safer Internet Centre.

2. Scope

This policy applies to all Staff Power Training (SPT) employees, learners, agency workers, contractors, volunteers, visitors, and any third party acting on behalf of SPT. It applies whether social media is accessed using SPT-owned equipment, personal devices, or third-party systems.

For the purposes of this policy, "social media" includes, but is not limited to:

· Social networking sites (e.g. Facebook, Instagram, Threads, X/Twitter).
· Professional networking platforms (e.g. LinkedIn).
· Video-sharing platforms (e.g. YouTube, TikTok, Vimeo).
· Online forums, discussion boards, blogs and comment sections.
· Messaging and communication platforms where content can be shared publicly or within groups (e.g. WhatsApp, Facebook Messenger, Discord, Telegram and similar applications).
· Any future digital platform that enables users to create, share, comment on or exchange content electronically.

This policy applies to:

· Official SPT social media accounts.
· Personal social media accounts where an individual identifies themselves as connected to SPT or where their activity may reasonably be associated with SPT.
· Public and private social media groups.
· Social media activity undertaken during working hours and, where relevant, outside working hours where such activity may impact SPT, its learners, staff, partners or reputation.

The policy should be read alongside the Safeguarding Policy, Data Protection Policy, Acceptable Use Policy, Staff Code of Conduct, Learner Behaviour Policy and Disciplinary Procedures.

3. Roles and Responsibilities

Directors and Senior Leadership Team

The Directors and Senior Leadership Team are responsible for:

· Ensuring appropriate governance and oversight of SPT's social media activity.
· Approving official organisational social media accounts.
· Ensuring adequate resources and training are available to support safe and responsible social media use.

· Taking appropriate action where serious breaches of this policy occur.
· Authorising the creation of official social media accounts.
· Monitoring compliance with this policy.
· Supporting investigations into reported concerns and policy breaches.
· Ensuring social media activity aligns with organisational values and objective.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead is responsible for:
· Managing safeguarding concerns arising from social media activity.
· Recording, investigating and escalating concerns where appropriate.
· Providing advice and guidance regarding online safety risks.
· Liaising with external agencies when required.

Staff

All staff members are responsible for:
· Complying with this policy and related organisational procedures.
· Maintaining professional boundaries with learners online.
· Protecting confidential and personal information.
· Reporting safeguarding, wellbeing, security or reputational concerns promptly.
· Using official social media accounts only when authorised to do so.

Learners

Learners are responsible for:
· Using social media respectfully and responsibly.
· Refraining from cyberbullying, harassment or discriminatory behaviour.
· Respecting the privacy and rights of other learners, staff and partners.
· Reporting concerns or inappropriate online activity to a member of staff.

Account Administrators

Individuals authorised to manage official SPT social media accounts are responsible for:
· Ensuring content is accurate, professional and compliant with this policy.
· Protecting account credentials and security settings.
· Promptly removing inappropriate content where lawful and appropriate to do so.
· Reporting suspected account compromise, security incidents or inappropriate activity immediately.

4. Key Legislation and Guidance

4.1 This policy is written in accordance with:
- Keeping Children Safe in Education (KCSIE)

- The Prevent Duty
- UK General Data Protection Regulation (UK GDPR)
- Guidance from the UK Safer Internet Centre and the NSPCC

5. Key Principles of the Online Safety Policy

5.1 The policy is built around a commitment to four key principles:
- Empowerment: Equipping learners and staff with the knowledge and skills to use technology safely and responsibly.
- Protection: Implementing technical and procedural safeguards to protect users from online harm.
- Inclusion: Ensuring that all members of our community can access online resources and support without fear of discrimination or harassment.
- Accountability: Establishing clear roles, responsibilities, and reporting mechanisms to address any online safety incidents effectively.

6. Official Social Media Use

All official social media accounts representing Staff Power Training (SPT) must be approved by the Senior Leadership Team. Official accounts must only be managed by authorised individuals acting on behalf of SPT.

Content published through official accounts must be professional, accurate, lawful and aligned with SPT's values, objectives and brand identity. All users of official accounts are responsible for ensuring compliance with this policy and any associated organisational procedures.

Engagement with learners, employers, stakeholders and members of the public must be conducted respectfully, professionally and in a timely manner.

7. Social Media Content Standards

All content published on official SPT social media accounts, and any content posted through personal accounts that may reasonably be associated with SPT, must comply with the following standards.

Acceptable Content

Social media may be used to:

· Promote training programmes, events and organisational achievements.
· Share relevant educational, industry and employment-related information.
· Celebrate learner and staff success where appropriate consent has been obtained.
· Support engagement with learners, employers, partners and the wider community.
· Promote safeguarding, wellbeing, equality, diversity and inclusion initiatives.

Prohibited Content

The following content must not be published:
· Confidential, commercially sensitive or restricted information.
· Personal data without appropriate consent or lawful basis.
· Defamatory, threatening, abusive, offensive, discriminatory or harassing content.
· Material that may constitute bullying, intimidation or victimisation.
· Copyrighted material used without permission.
· False, misleading or unverified information.
· Unauthorised statements made on behalf of SPT.
· Content that may bring SPT, its learners, staff, employers or partners into disrepute.
· Content that breaches safeguarding, equality, diversity, inclusion or data protection requirements.

Use of Branding

The SPT name, logo and branding may only be used for authorised business purposes. Staff and learners must not create social media accounts that appear to represent SPT without prior approval from the Senior Leadership Team.

Responding to Online Activity

Individuals managing official accounts should respond to comments and enquiries professionally and courteously. Staff must not engage in arguments, abusive exchanges or inappropriate discussions on behalf of SPT. Concerns, complaints or safeguarding matters identified through social media should be managed through the appropriate organisational procedures.

8. Personal Social Media Use

SPT respects the right of staff and learners to use personal social media accounts. However, individuals should be aware that their online activity may affect SPT's reputation where an association with the organisation can be identified.

When using personal social media accounts, staff and learners must:
· Maintain appropriate standards of professionalism and respect.
· Protect confidential, commercially sensitive and personal information.
· Avoid posting content that could damage the reputation of SPT or negatively affect its learners, staff, employers or partners.
· Maintain professional boundaries and avoid inappropriate online relationships or communication with learners.
· Comply with safeguarding, equality, diversity, inclusion and data protection requirements.

Where staff discuss work-related matters on personal accounts, they are encouraged to make it clear that any views expressed are their own and do not represent the views of SPT. An example disclaimer is:

"The views expressed are my own and do not necessarily reflect those of my employer."

Staff are advised not to accept social media connection requests from learners on personal accounts where doing so may compromise professional boundaries or create safeguarding concerns. Communication with learners should normally take place through approved organisational channels.

9. Reputational Risk and Professional Conduct

SPT recognises that social media activity, whether undertaken through official or personal accounts, can have an impact on the organisation's reputation, relationships and public confidence. Staff and learners are therefore expected to conduct themselves online in a manner that reflects SPT's values and professional standards.

Individuals must not:

· Post content that could reasonably be considered damaging to the reputation of SPT, its learners, staff, employers, partners or stakeholders.
· Make false, misleading or malicious statements about SPT or individuals associated with the organisation.
· Engage in online behaviour that could undermine professional relationships or public confidence in SPT.
· Present personal opinions as official SPT views without authorisation.
· Use SPT branding, logos or materials in a way that suggests official endorsement where no such approval exists.

SPT respects the right of individuals to express personal views and participate in lawful online activities. However, where social media activity negatively affects the organisation, its reputation, working relationships, safeguarding responsibilities or legal obligations, appropriate action may be taken in accordance with relevant organisational policies and procedures.

10. Safeguarding and Online Safety

10.1 Confidentiality: Do not disclose any confidential information about SPT, its staff, learners, or partners. This includes financial information, personal data, and unpublished business strategies.

10.2 Respect and Professionalism: Do not post defamatory, harassing, discriminatory, or obscene content. Be respectful in all online interactions, even when disagreeing with others.

10.3 Disclaimers: If discussing work-related matters, it is advisable to include a disclaimer stating that the views expressed are personal and do not represent the official position of SPT. For example: "The views expressed are my own and do not necessarily reflect the views of my employer/training provider."

10.4 Boundaries: Staff are advised against accepting friend or connection requests from learners on their personal social media accounts to maintain professional boundaries. All communication with learners should be through official channels.

SPT is committed to promoting a safe, respectful and inclusive online environment for learners, staff and stakeholders. All users of social media must behave responsibly and take reasonable steps to

protect themselves and others from online harm. This policy should be read in conjunction with SPT's Safeguarding Policy and Data Protection Policy.

Inappropriate Contact

Any online contact, communication or behaviour involving a learner, member of staff or third party that is inappropriate, concerning or potentially harmful must be reported immediately to the Designated Safeguarding Lead (DSL). All concerns will be treated seriously and managed in accordance with SPT's safeguarding procedures.

Images, Videos and Consent

Written consent must be obtained before publishing photographs, videos or recordings of learners, staff or visitors on social media platforms, websites or promotional materials. All images and videos must be used appropriately and in accordance with SPT's Data Protection Policy and Privacy Notice.

Individuals may withdraw their consent at any time. Where consent is withdrawn, SPT will take reasonable steps to remove content from future use and from platforms under its control where practicable.

Images and videos must not contain personal, confidential or sensitive information that could place an individual at risk or breach their privacy.

Cyberbullying and Online Harassment

SPT has a zero-tolerance approach to cyberbullying, online harassment, intimidation, discrimination or abusive behaviour. Any allegations or reports of such behaviour will be investigated and may result in disciplinary action, termination of a learning agreement, or referral to external agencies where appropriate.

Reporting Online Safety Concerns

Any concerns relating to online safety, social media activity, cyberbullying, inappropriate contact or safeguarding risks should be reported without delay through the appropriate reporting procedures. SPT will respond promptly, sensitively and confidentially to all reported concerns.

11. Data Protection (GDPR)

All social media activity must comply with the Data Protection Act 2018 (including the UK General Data Protection Regulation).

- Personal Data: Do not share any personal data of staff, learners, or third parties without their explicit consent.

- Privacy Settings: Users are encouraged to use appropriate privacy settings on their personal social media accounts to control who can see their information.

12. Reporting a Concern

Any learner or member of staff who has an online safety, safeguarding, security or social media-related concern should report it to a member of staff as soon as possible. Concerns will be escalated to the Designated Safeguarding Lead (DSL), Senior Leadership Team or other appropriate manager depending on the nature of the issue.

All reports will be:

· Taken seriously and treated sensitively.
· Recorded and assessed appropriately.
· Investigated promptly and proportionately.
· Handled in a confidential manner, subject to safeguarding and legal requirements.

Where necessary, SPT may:

· Remove or request the removal of inappropriate content.
· Restrict access to organisational social media accounts.
· Initiate disciplinary procedures.
· Refer safeguarding concerns to the appropriate authorities or agencies.
· Report criminal activity, harassment, threats or unlawful conduct to the police or relevant regulatory bodies.

Individuals raising concerns in good faith will not suffer any detriment for reporting genuine issues.

If required, online safety concerns can also be reported via the UK Safer Internet Centre Report Harmful Content service:
https://reportharmfulcontent.com/harms

13. Breaches of Policy

13.1 Any breach of this social media policy may result in disciplinary action, up to and including dismissal for staff or termination of the learning agreement for learners.

13.2 In serious cases, a breach may be reported to the relevant authorities.

14. Further Guidance

For further information or clarification on any aspect of this policy, please contact:

Jonathan Hall - Director of Continuous Improvement

Mackies Corner Floor 2

High Street West Sunderland

SR1 1TX

T: 0191 500 3777

E: jonathan.hall@staffpowergroup.com

15. Policy Review

This policy has been developed with reference to the following legislation and guidance:

· Data Protection Act 2018

· UK General Data Protection Regulation (UK GDPR)

· Equality Act 2010

· Online Safety Act 2023

· Prevent Duty Guidance

· UK Safer Internet Centre Guidance

· NSPCC Online Safety Guidance

SPT will review this policy periodically to ensure continued compliance with relevant legislation, regulatory requirements and recognised good practice.