Social Media Policy

Policy Reference	IT007
Author	Information Technology Director
Policy Agreed (date):	October 2025
Next Review (date):	January 2027
Approved by:	Central Leadership Team

Contents

Version Control

Version	Author	Date	Changes
V 1.0	Director of Information Governance & Compliance	October 2025	First draft
V 1.1	Director of Information Governance & Compliance	December 2025	GDPR statement inserted into policy. Inclusion of reference to Online Safety policy. Clearly explained the definition of social media. Amended specific references of 'Facebook' to 'Official Social Media Accounts'. Included statement around professional boundaries under the title 'Personal Use of Social Media by Staff'. Included Appendices I/II - Privacy settings checklist and incident response flowchart.
V 1.2	HR Director	January 2026	References to Deputy Headteacher and Executive Headteacher to be read as Managing Director and Executive Leadership Team is Central Leadership Team. All policies to be updated by July 2026.

1. Purpose & scope

This Social Media Policy sets out clear expectations and rules for the safe, responsible, and lawful use of social media by all members of the provision community. Its purpose is to:

- Protect learners, staff, parents/carers, and the wider community
- Safeguard children and young people, particularly those who are vulnerable
- Ensure compliance with UK GDPR, data protection, safeguarding, and online safety requirements
- Protect the reputation and integrity of the provision

This policy applies to:

- All staff (including governors, volunteers, agency staff, and contractors)
- Learners
- Parents and carers

The policy applies to both professional and personal use of social media, whether during working hours or outside of them, and regardless of the device used.

This policy should be read in conjunction with the following:

- Safeguarding and Child Protection Policy
- Data Protection Policy and Privacy Notices
- Staff Code of Conduct
- Behaviour Policy
- Online Safety Policy
- ICT Acceptable Use Policy

All members of the provision should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection legislation. Everyone must also operate in line with the provision's equalities, harassment, child protection, safer recruitment, and online safety and ICT acceptable use policies.

2. Definition of Social Media

For the purpose of this policy, social media refers to any online platform or technology that enables users to communicate, share content, or interact with others. This includes, but is not limited to:

- Social networking sites (e.g. Facebook, Instagram, TikTok)
- Messaging and group chat services (e.g. WhatsApp, Snapchat, Discord)
- Video and livestreaming platforms (e.g. YouTube, Twitch)
- Gaming platforms with communication functions
- Blogs, forums, and comment sections
- AI-generated content and image-sharing tools

This list is non-exhaustive and includes emerging platforms.

3. Data Protection, Privacy and Consent

All use of social media must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- Personal data relating to learners, staff, or parents/carers must **never** be shared without a lawful basis.
- Images, videos, or names of learners may only be shared on official provision social media channels where **explicit written consent** has been obtained from the parent/carer (and the learner where appropriate).
- Consent is always:
    - Freely given, specific, informed, and unambiguous
    - Recorded and stored securely
    - Capable of being withdrawn at any time

The provision will not:

- Tag learners or parents/carers
- Enable facial recognition features
- Share location data
- Identify learners as having SEN, EHCPs, or other vulnerabilities

Any breach or concern relating to data protection must be reported immediately to the Director of Information Governance & Compliance.

4. Use of official provision social media

The provision's official social media presence is limited to:

Facebook: The Bridge Alternative Provision – Clifton Centre (www.facebook.com/tbap)

These accounts are managed solely by the Managing Director and the Director of Information Governance & Compliance. No other staff member may access, manage, or post content unless formally authorised.

If you have suggestions for something you'd like to appear on our provision social media channel(s), please speak to the Director of Information Governance & Compliance.

Content posted may include:

- Operational updates and alerts
- Reminders and key dates
- Events, activities, and achievements (with consent)
- Job vacancies
- Links to newsletters, guidance, and official resources
- Invitations for feedback

The provision **will not** post on Facebook:

- Identifiable images or names without consent

- Messages directed at individual users
- Political content
- Commercial advertising unrelated to the provision
- Links to staff personal accounts

Moderation

Official social media accounts are moderated regularly. Staff responsible for our social media accounts will delete as soon as reasonably possible:

- Abusive, racist, sexist, homophobic or inflammatory comments
- Comments we consider to be spam
- Personal information, such as telephone numbers, address details, etc.
- Posts that advertise commercial activity or ask for donations

Every reasonable effort will be taken to politely address concerns or behaviour of individual users, following the provision's complaints policy. If users are repeatedly abusive or inappropriate, they will be blocked.

Staff responsible for our social media accounts will also ensure that all content shared on social media platforms is age appropriate for the provision community.

Following other social media users

The provision does not endorse any external accounts or content it follows or interacts with.

5. Personal use of social media by staff

The provision expects all staff (including governors and volunteers) to maintain professional boundaries online at all times. Privacy settings do not remove professional accountability. The provision further expects staff to consider the safety of learners and the risks (reputational and financial) to the provision when using social media channels, including when doing so in a personal capacity. Staff are also responsible for checking and maintaining appropriate privacy and security settings of their personal social media accounts.

Staff members will report any safeguarding issues they become aware of through the correct channels.

When using social media, staff must not:

- Use personal accounts to conduct provision business
- Accept or initiate contact with current or former learners via personal social media
- Share images or information about learners, staff, or parents/carers
- Post content that could undermine safeguarding, trust, or the reputation of the provision
- Express views that could reasonably be interpreted as representing the provision
- Link personal social media accounts to provision email addresses
- Use personal social media during timetabled teaching time

Any concerns regarding a member of staff's personal use of social media will be dealt with in line with the staff behaviour policy.

Any communication received from current learners (unless they are family members) on any personal social media accounts must be reported to the designated safeguarding lead (DSL) or member of the senior leadership team immediately.

Staff should also not have contact via personal accounts with past learners (if ongoing communication is required, this should be carried out by using official provision channels).

6. Personal use of social media by learners

The provision encourages learners to

- Be respectful to members of staff, and the provision, at all times
- Be respectful to other learners and parents/carers
- Protect their own privacy and safety
- Direct any complaints or concerns through the provision's official channels, so they can be dealt with in line with the provision's complaints procedure

Learners should not use social media to:

- Complain about individual members of staff
- Complain about the provision
- Make inappropriate comments about members of staff, other learners or parents/carers
- Post images of other learners without their permission

Any concerns about a learner's social media use will be dealt with in line with the provision's behaviour policy.

7. Personal use of social media by parents/carers

The provision expects parents/carers to help us model safe, responsible and appropriate social media use for our learners.

When communicating with the provision via official communication channels, or using private/independent channels to talk about the provision, parents and carers should:

- Be respectful towards, and about, members of staff and the provision at all times
- Be respectful of, and about, other parents/carers and other learners and children
- Direct any complaints or concerns through the provision's official channels, so they can be dealt with in line with the provision's complaints procedure

Parents/carers should not use social media to:

- Complain about individual members of staff, other parents/carers or learners
- Complain about the provision
- Make inappropriate comments about members of staff, other parents/carers or learners
- Draw attention to, or discuss, behaviour incidents
- Post images of children other than their own

Concerns or complaints must be raised through official provision channels. Where social media use causes safeguarding, reputational, or staff welfare concerns, the provision reserves the right to take further action.

WhatsApp groups

The provision does not permit the use of WhatsApp or similar messaging platforms for official communication.

Any parent- or learner-led messaging groups operate independently and are not monitored or managed by the provision. Such groups must not be used to discuss learners, staff, or incidents.

8. Training & awareness

The PSHE curriculum will deliver specific lessons relating to Social Media throughout the year for learners. Guidance and awareness infographics will be delivered to parents/carers regularly via email. As well as staff being provided our Social Media policy during induction, staff will also be updated throughout the year on changes to this policy, and provided training throughout the year during weekly CPD sessions.

9. Monitoring & reviewing

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes. This includes ascertaining and demonstrating that expected standards are being met by those using the systems, and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

The Managing Director will monitor the implementation of this policy, including making sure that it is updated to reflect the needs and circumstances of the provision.

This policy will be reviewed every year by the Director of Information Governance & Compliance.

The Central Leadership Team is responsible for approving this policy.

Appendix I - Social Media Incident Response Flowchart

This flowchart outlines the required steps when a social media incident involving learners, staff, parents/carers, or the provision is identified.

Step 1: Identify the Incident

An incident may include:

- Safeguarding concerns (e.g. contact from unknown adults, grooming, threats)
- Inappropriate or abusive content
- Sharing of personal data or images without consent
- Defamatory or harmful comments about the provision or individuals
- Staff–learner boundary breaches

Any member of staff who becomes aware of an incident must act immediately.

Step 2: Assess Immediate Risk

Ask:

- Is a learner at immediate risk of harm?
- Does the content involve safeguarding, exploitation, or threats?

If YES:

- Report immediately to the Designated Safeguarding Lead (DSL)
- Preserve evidence (screenshots, URLs, timestamps)
- Do NOT engage online or attempt to resolve independently

If NO:

- Proceed to Step 3

Step 3: Preserve Evidence

- Take screenshots (including usernames, dates, and platform)
- Record where the content appeared and who reported it
- Do not comment, like, or share the content

Step 4: Report Internally

Report the incident to:

- DSL (for safeguarding concerns)
- Director of Information Governance & Compliance (for data protection, reputational, or staff conduct issues)
- Managing Director where appropriate

Step 5: Decide Response Route

The Central Leadership Team will determine the appropriate action, which may include:

- Safeguarding referral (Children's Services / Police / LADO)
- Data breach assessment and ICO consideration
- Requesting removal of content
- Blocking or reporting users to the platform
- Initiating the complaints procedure
- Staff disciplinary procedures

Step 6: Record and Review

- Record the incident and actions taken
- Review whether policy, training, or controls need strengthening
- Provide appropriate support to affected individuals

Appendix II - Social Media Privacy Settings Checklist

This checklist supports staff in maintaining safe and appropriate use of personal social media accounts.

Account Visibility

- [ ] Profile set to private where possible
- [ ] Past posts reviewed for appropriateness
- [ ] Search engine visibility limited

Connections and Contacts

- [ ] No current or former learners added as friends or contacts
- [ ] No learner-related group chats
- [ ] Unknown contacts reviewed and removed

Content and Sharing

- [ ] No images of learners shared
- [ ] No references to provision incidents, learners, or families
- [ ] No posts that could undermine safeguarding or professional trust

Tagging and Mentions

- [ ] Tagging disabled or restricted
- [ ] Timeline review enabled
- [ ] Location tagging switched off

Messaging and Comments

- [ ] Direct messages restricted where possible
- [ ] Auto-delete or archive settings reviewed
- [ ] Comments monitored and inappropriate interactions reported

Security

- [ ] Strong, unique passwords in use
- [ ] Two-factor authentication enabled
- [ ] Devices secured with passcodes/biometrics

Professional Boundaries

- [ ] Personal opinions clearly separated from professional role

- [ ] Work email not linked to social media accounts
- [ ] No assumption of anonymity online

Staff are reminded that privacy settings reduce risk but do not remove professional accountability.