TRUE LEARNING

PARTNERSHIP

SOCIAL MEDIA POLICY	
Policy Ref Number: TTLP/52	**Reviewed by: Director of ICT and Networks** **Approved by People Committee**
Policy Date: June 2025	**Review Date: June 2028**

Summary

This document outlines the social media policy for True Learning, establishing guidelines for the use of social media by staff, students, and parents/carers. It emphasises the importance of respectful communication and compliance with safeguarding and data protection policies.

- **Purpose and Scope:** The policy sets rules for the usage of social media channels, aiming to ensure safe online engagement within the school community. 1 2
- **Official School Social Media Use:** The school communicates through platforms like Facebook and prohibits unauthorised access to official accounts. 3 4
- **Staff Personal Use of Social Media:** Staff must maintain professionalism and privacy, avoiding personal interactions with students and not using personal accounts for school business. 5 6
- **Pupil Social Media Use:** Pupils are encouraged to be respectful and direct concerns through official channels, refraining from negative comments about staff or the school on social media. 7 8
- **Parent/Carer Social Media Use:** Parents/carers are expected to model appropriate online behaviour and should communicate respectfully, avoiding complaints about the school on social media. 9 10
- **Monitoring and Review:** The school reserves the right to monitor social media use for compliance and will review the policy annually. 11 12

Significant changes:

- To only use Facebook and move away from X (Twitter), this will be reviewed annually
- A form to allow staff to report offensive or defamatory Content
- Not using WhatsApp to communicate about trust business on personal phones.

Contents

1. Purpose and scope 4
2. Use of official school social media 4
2.1 Social Media Platforms 4
2.3 Moderation 5
3. Personal use of social media by staff 5
4. Personal use of social media by pupils 6
5. Personal use of social media by parents/carers 6
6. Monitoring and review 7
6.1 Offensive or Defamatory Content 7
6.2 No Tolerance for Harassment 8
7. Related policies 8

1. Purpose and scope

This policy aims to:

- Set guidelines and rules on the use of the trust's social media channels
- Establish clear expectations for the way members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding

Staff, students and parents/carers are required to read, understand and comply with this social media policy. This policy applies to the use of social media for business and personal purposes, whether during school working hours or otherwise.

It applies regardless of whether the social media is accessed using:

- School IT facilities and equipment
- Equipment belonging to members of staff and pupils
- Any other IT/Internet-enabled equipment

All members of the school 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 school's equalities, harassment, child protection, safer recruitment, and online safety and ICT acceptable use policies.

1.1 Definition of social media

For the purposes of this document, 'social media' is considered to include all technologies that allow individuals to communicate and share information (including photos and video), including group messaging services such as WhatsApp.

2. Use of official school social media

True Learning regularly communicates through various online channels.

The school's official social media channels are as follows:

- Facebook

Staff members who the school or central team has not authorised to manage or post to the account must not access or attempt to access these accounts.

Please do not use WhatsApp to communicate Trust or work business with colleagues on personal devices.

Please speak to your line manager if you have suggestions for something you'd like to appear on our school or trust social media channel(s).

2.1 Social Media Platforms

The trust will post on social media platforms:

- Alerts about changes (e.g. changes to procedures, severe weather updates, staffing changes)

- Reminders (e.g. approaching deadlines, events or class activities, reminders about policies/procedures)
- Advertisements for school events or activities
- Job vacancies or requests for volunteers
- Links to newsletters, guidance and factsheets for parents and carers
- Achievements of pupils and staff
- Photos or posts about school trips, events and activities
- Seasonal greetings and messages about religious festivals
- Invitations to provide feedback

The trust **will not** post on social media platforms:

- Names and photos of individuals (unless they have given consent)
- Full names and photos of students
- Harmful or abusive comments
- Messages to specific people
- Political statements
- Advertisements for businesses unless directly related to the school or trust
- Links to staff members' personal accounts

2.3 Moderation

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 trusts 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 school community.

2.4 Following other social media users

The trust/school:

- Will only 'like' Facebook pages with a non-commercial interest – being 'liked' by us doesn't imply endorsement of any kind

3. Personal use of social media by staff

The school expects all staff (including governors and volunteers) to consider the safety of pupils and the risks (reputational and financial) to the school 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.

When using social media, staff **must not**:

- Use personal accounts to conduct school business
- Accept 'friend requests' from, or communicate with, pupils past or present
- Complain about the school, individual pupils, colleagues or parents/carers
- Reference or share information about individual pupils, colleagues or parents/carers
- Post images of pupils
- Express personal views or opinions that could be interpreted as those of the school
- Link their social media profile to their work email account
- Use personal social media during timetabled teaching time except in a professional capacity

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 pupils (unless they are family members) on any personal social media accounts will be reported to the designated safeguarding lead (DSL) or member of the senior leadership team immediately.

Staff should not have contact via personal accounts with past pupils (if ongoing communication is required, this should be using via official school channels).

4. Personal use of social media by pupils

The trust encourages pupils to

- Be respectful to members of staff, and the trust, at all times
- Be respectful to other pupils and parents/carers
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

Pupils **should not** use social media to:

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

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

5. Personal use of social media by parents/carers

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

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

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

Parents/carers **should not** use social media to:

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

6. Monitoring and review

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 trust executive team and senior leadership team will monitor the implementation of this policy, including ensuring that it is updated to reflect the school's needs and circumstances.

This policy will be reviewed annually.

6.1 Offensive or Defamatory Content

We recognise that social media is a public space and that online content can sometimes be harmful. If you come across any social media posts that you believe to be offensive, defamatory, or damaging to your reputation, the school or trusts reputation, or any other individual or group associated with the trust, we ask that you report it immediately.

How to report it:

- Document the content (screenshot, note down the link, or provide a description of the post).
- Complete the Reporting Form: Visit https://forms.office.com/e/gxx4E2aRVi. Please include all relevant details, including the nature of the post, the platform it was found on, and any other information that can assist us in addressing the issue.
- Remain Professional: Refrain from engaging directly with the offensive post. We recommend leaving the matter to the appropriate channels for investigation and resolution.

6.2 No Tolerance for Harassment

We have a zero-tolerance policy for harassment or defamatory behaviour in both the workplace and online. We will investigate any reported issues promptly and take appropriate action to resolve the situation.

7. Related policies

- School safeguarding Policy
- Trust ICT and internet acceptable use policy
- School Behaviour policy
- Trust Staff Code of Conduct
- Trust Mobile phone use policy

Prevent your account from being hacked

Enable Two-Factor Authorisation (2FA) log-in: this functionality will request you to insert a security code anytime you log in.

Please note that 2FA log-in via text message is only available to X Premium subscribers. Accounts that aren't subscribed to X Premium are still able to link their account to an authentication app such as Google Authenticator or Duo Mobile, or a physical key. How to review: Settings & Privacy > Security > Two Factor Authentication

Use a long password of 15–20 characters that includes numbers, uppercase and lowercase and special characters. This works better with a password management tool.

Set up password protection

This functionality prompts to enter either your email address or phone number, or your email address then phone number if both are associated with your account to send a reset password link or confirmation code if you ever forget it.

How to review: Settings & Privacy > Security > Additional password protection > Password reset protect

Review third party apps that have access to your account and revoke access to the ones you are not actively using.

How to review: Settings & Privacy > Apps & Sessions > Connected Apps