JOHN TAYLOR MULTI ACADEMY TRUST

Social Media Policy

Implementation date: February 2026

Next Review Date: March 2027

Policy Owner: Rachel Snary - Trust Marketing Manager

1. Purpose

This policy sets out expectations, responsibilities and standards for staff use of social media in both professional and personal capacities where their actions could affect the Trust, its schools, pupils, parents or colleagues. It aims to:

- protect pupils, staff, school and the Trust's reputation;
- support safe, professional use of social media for engagement and learning; and
- ensure compliance with safeguarding, confidentiality and data-protection obligations.

This policy should be read in conjunction with:

- Staff Code of Conduct Policy
- Staff Disciplinary Policy
- Data Protection/GDPR Policy
- IT Acceptable use Policy
- Health & Safety Guidance
- Trust Issued Social Media Guidance

Policy Source and Development Statement

This Social Media Policy has been developed using a range of reputable sources to ensure it reflects current best practice in safeguarding, data protection, professional conduct, and the appropriate use of digital communication within UK education settings. Guidance from national authorities and expert organisations has been incorporated throughout, including relevant advice from the Information Commissioner's Office (ICO) on data protection and the use of images in schools, Department for Education (DfE) materials on online safety, and NSPCC guidance on safe staff–pupil boundaries in digital and social media contexts. In addition, this policy is based on Teacher/HR Standards, the Nolan principles and the JTMAT Code of Conduct.

Collectively, these sources have informed the structure, expectations, and safeguards set out in this policy, ensuring it is robust, legally compliant, and aligned with recognised sector standards. The policy will be reviewed periodically to reflect changes in technology, legislation, and professional practice.

2. Scope

This policy applies to use of personal, school and Trust accounts on any platform that constitutes social media (including but not limited to: Facebook, Twitter/X, Instagram, TikTok, Snapchat, WhatsApp, YouTube, LinkedIn, blogs, forums, and comment sections) at any time in school hours or beyond and from any device.

3. Definitions

Social media: websites, platforms, apps and other online spaces used for sharing content and communicating.

Professional account: accounts created by or on behalf of the Trust/school for official communications.

Personal account: accounts used by staff in a personal and private capacity.

Device: any work or personal hardware used to access, construct and share social media content.

4. Roles & Responsibilities

- **Trust Board** - Sets strategic direction and approves Social Media Policy. Hold the Trust to account for compliance with relevant legislation.
- **Trust Marketing Manager** - Monitors implementation and risk management. Provides training, advice and guidance to school leaders on implementation and compliance in schools.
- **Headteachers** - Ensure staff have read and understand the policy and are clear about the professional expectations of using social media. Ensure compliance within their school and seeking advice and taking action when the policy is breached.
- **Staff** – Read, understand and follow this policy and associated documents e.g. Staff Code of Conduct, use social media safely and, report concerns.

5. Monitoring & Review

This policy will be reviewed at least annually, or sooner if statutory guidance changes or a relevant incident prompts review.

6. Core Principles

All employees must:

- Act professionally, model appropriate behaviour and remember that they are ambassadors of the Trust and their school at all times.

- Keep professional and personal accounts separate where possible. Where this is not possible, staff must manage privacy settings and content accordingly.

- Not identify themselves as employees of the Trust or any school named within it on personal accounts (other than LinkedIn)

- Not identify themselves online as speaking on behalf of the Trust or their school unless expressly authorised. Staff must not create the impression they represent official Trust or their school positions on personal accounts.

- Avoid posting content that could bring the Trust or their school into disrepute (defamation, bullying, harassment, discriminatory content, obscene, upsetting or illegal material).

7. Professional use of social media (official accounts)

- All official Trust/school social media accounts must be approved by /Headteacher/CEO. Accounts should have named administrators and at least two relevant senior leaders with access.

- Content must safeguard pupils' privacy and welfare: do not publish pupil names with photos unless valid consent is recorded and stored according to the Trust's data-protection procedures. Follow ICO guidance on photography and consent.

- Official posts must be professional, accurate and non-partisan. Posts that respond publicly to complaints or sensitive issues should be led by Senior Leadership Team.

- Keep a simple published records/log of posts and admin changes for transparency (who posted, when, content summary).

- The Trust publishes guidance to school on corporate use of social media.

8. Personal use and boundaries

- Staff should not communicate with pupils (including ex-pupils under the age of 18), or follow/friend them or their parents/carers, from personal accounts. All communications with pupils and parents/carers should be via Trust-provided channels or official accounts. (There are narrow exceptions for pre-existing family relationships; discuss with HR/DSL.)

- Do not share confidential or commercially sensitive information on personal accounts (trust/school business, staffing matters, pupil details or information about third parties).

- If a member of staff is the subject of abusive or defamatory comments online related to their role, they should inform their line manager or HR; the Trust will support staff subjected to harassment because of their employment.

- Think before you post: remember posts may be shared in full or cropped/edited beyond intended audiences; even deleted posts can be archived or screenshotted – this applies to text, and images shared equally.

- Social Media posts or images could be viewed against Staff Code of Conduct Policy.

Professional images produced or commissioned by the Trust or school must not be shared on personal social media accounts, as this may raise safeguarding and data protection concerns.9. Safeguarding, confidentiality & data protection

- **Safeguarding first**: any concerns (e.g., child sexual exploitation, grooming, explicit material) seen on social media must be reported immediately to the Designated Safeguarding Lead (DSL) and follow the Trust safeguarding procedures.

- **Data protection**: processing of pupil or staff personal data via social media must comply with UK GDPR. Do not publish images, attendance details, staffing records, or pupil assessment information without lawful basis and recorded consent where required. Follow ICO school resources for privacy and children's data.

- **Photographs and video**: obtain and record parental/guardian/staff consent for the use of pupils' images in Trust materials and on social media according to the Trust's consent process. Where consent is not granted, ensure pupils are not identifiable.

10. Communicating with parents and the community

- Official channels should be used for school announcements and engagement. Staff must not post disciplinary or sensitive matters about parents, pupils, colleagues or other professionals on personal accounts. If parents contact staff via social media, staff should direct them to official school channels.

11. Use of Trust equipment and working time

- Use of Trust devices and networks for personal social media during working hours should be in line with the Trust's acceptable use policy (e.g., limited at break times). Personal use must never interfere with duties.

12. Recruitment

It is prohibited for any employee of the Trust, particularly panel members either themselves or via a third party to conduct searches on applicants or candidates on social media or the internet, outside of the parameters permitted in the Online Search set out in Keeping Children Safe in Education. The relevant professional will undertake this search on shortlisted external candidates, and any publicly reported and relevant matters will be dealt with in accordance with statutory and Trust guidance.

13. Intellectual Property

Learning resources and administrative documents—including, but not limited to, frameworks of effectiveness, guidance documents, and internal operational materials—are produced for use within our schools and must not be posted or shared on public or general-access online platforms, including social media. Colleagues are prohibited from publishing such materials externally unless explicit written authorisation has been granted.

14. Monitoring, reporting & breach handling

- The Trust reserves the right to monitor official accounts and may need to review public online content which mentions the Trust where there are legitimate concerns about safeguarding or reputation. Monitoring of individuals' personal accounts will only be carried out where there is a lawful reason (e.g., safeguarding or disciplinary investigation) and in line with data-protection law.

- This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

- Where it is necessary to limit damage and/or protect the safety and reputation of any individual or entity, the Trust may contact website or social media host companies to request the removal of content.

- **Reporting**: staff must report any suspected policy breach, safeguarding concern or data-protection incident to their line manager/HR and DSL immediately.

- **Investigation**: Any suspected breach of this policy will lead to an appropriate level of investigation and any staff involved will be required to co-operate with that investigation, including reviewing social media accounts, requesting relevant passwords and login details for work equipment or accounts, the deletion of posts/accounts and/or the disabling of accounts.

- **Consequences**: breaches of this policy may lead to disciplinary action up to and including dismissal; unlawful conduct may be referred to statutory agencies. Examples of breaches include sharing confidential pupil data, contacting pupils via personal accounts, posting discriminatory or harassing content, or impersonating the Trust online.

  Whilst the Trust and its schools may endeavour to protect colleagues from external criticism and scrutiny, all employees must appreciate the limitations it has over editorial control and dissemination on social media platforms.

Appendix 1 – Rule for use of Social Media - Summary

Where staff choose to use social media, both whilst in the workplace and in their personal use they must observe the following rules:

- Staff must not publish any content that may directly or indirectly bring John Taylor MAT Academies' reputation into disrepute or negatively alter the public perception of the Trust
- Staff must not disclose or comment on commercially sensitive, anti-competitive, private or confidential information
- Staff must not post disparaging or defamatory statements about:
    - *The Trust*
    - *Current, past or prospective staff*
    - *Current, past or prospective pupils*
    - *Parents, carers or families*
    - *The Trust's suppliers and services providers; and*
    - *Other affiliates and stakeholders.*
- Staff must avoid posting comments about organisation-related topics such as MAT performance or Academy matters.
- Staff must not use MAT logos or photos including individual Academy logos, slogans or other trademarks without prior written permission.
- Staff must not use a work email address to sign up to any personal social media account.
- If Staff are using social media, they should make it clear in posts that they are speaking on their own behalf and that their views do not represent those of the Trust.
- Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.
- Staff must not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Staff must not use their personal accounts to contact parents/carers, family members or children/young people supported by MAT on any social media site. Direct messages from parents / carers or children /young people supported by MAT including friend requests that are received to staff member's personal social media accounts must either be declined or ask them to contact you using official channels of communication.
- Staff members are responsible for protecting the reputation of the Trust and are required to report any social media content they are aware of that disparages or reflects poorly on the Trust, its staff, pupils, parents, service providers or stakeholders - report this in the first instance to the headteacher without unreasonable delay.
- Staff must comply with the terms of use of specific social media platforms
- Staff must not escalate heated or private discussions, emails or correspondence and should be respectful to others. Staff are reminded where they feel uneasy about something they are about to publish, to refrain from publishing this.
- Staff must keep in mind the impact that their pictures, videos, shares and comments will have on the general perception of MAT by association and should be aware that any complaints which are received concerning this material may lead to an investigation. This includes comments that may be considered inflammatory and divisive, such as politics and religion.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with the Headteacher.