Frank Field
Education Trust

Social Media Policy and Procedure

Policy Information:

Date prepared	October 2026
Adopted by Board	October 2026
Implementation Date	Immediate
Frequency of Review	Bi-Annually
Review Date	October 2028

Approved by CEO:

Cath Green

Approved by Chair of Board:

David Wooff

Frank Field
Education Trust

Contents

Contents 2
1. Introduction and aims 3
2. Scope and status 3
3. Legal and regulatory framework 3
4. Roles and responsibilities 3
5. Core standards 4
6. Official Trust social media 4
7. Images, video, audio and personal data 4
8. Staff personal use and professional boundaries 5
9. Messaging applications and online groups 5
10. Safeguarding and online safety 6
11. Use during work and on Trust systems 6
12. Monitoring and access to information 6
13. Recruitment and online searches 6
14. Concerns, complaints and media enquiries 7
15. Breaches and fair response 7
16. Records, training and review 7
Appendix 1: Quick response guide 8

1. Introduction and aims

Frank Field Education Trust recognises that social media can support communication, professional learning and engagement with pupils, parents, carers, colleagues, and the wider community. It can also create safeguarding, confidentiality, data protection, security, employment, and reputational risks. This policy sets clear, proportionate expectations for official and personal use while respecting lawful private life and freedom of expression.

The policy aims to protect children and adults, maintain professional boundaries, ensure that Trust communications are accurate and accessible, safeguard personal and confidential information, and provide a fair framework for responding to concerns. It should be read alongside the Staff Code of Conduct, Child Protection and Safeguarding Policy, Online Safety Policy, ICT Acceptable Use Policy, Data Protection Policy, Records Management & Retention Schedules Policy, Whistleblowing Policy, Disciplinary Procedure and relevant communications or brand guidance.

2. Scope and status

This policy applies to employees, workers, agency and supply staff, apprentices, trainees, consultants, contractors, trustees, governors, volunteers, and any other adult acting for or representing the Trust or one of its academies. It applies to official accounts, work-related use, personal use that has a sufficiently close connection with the Trust or the person's role, and activity on or away from Trust premises.

The policy covers social networks, professional networking sites, blogs, forums, video and image-sharing services, livestreams, podcasts, messaging applications, group chats, collaborative platforms, review sites and comparable current or future services. Email is governed principally by the ICT Acceptable Use Policy, but the standards in this policy also apply where an online communication has a social or public-facing character.

This policy does not form part of any contract of employment. The Trust may amend it following appropriate consultation. Any action under the policy will take account of the facts, context, seriousness, impact and the individual's employment or other status.

3. Legal and regulatory framework

The Trust will apply this policy consistently with applicable law and guidance, including the UK General Data Protection Regulation; the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025; the Equality Act 2010; the Human Rights Act 1998; the Defamation Act 2013; the Copyright, Designs and Patents Act 1988; the Computer Misuse Act 1990; the Protection from Harassment Act 1997; the Public Interest Disclosure Act 1998; and relevant criminal law.

The Trust will also have regard to Keeping Children Safe in Education 2026, the Teachers' Standards, Department for Education guidance on data protection, filtering, and monitoring, Information Commissioner's Office guidance on employment practices and monitoring, and relevant safeguarding, online safety, and safer recruitment guidance. References to legislation include amendments and replacement provisions in force from time to time.

4. Roles and responsibilities

The Trust Board is responsible for approving the policy and seeking assurance that suitable safeguarding, data protection, and governance arrangements are in place. The Chief Executive Officer and Chief Finance & Operating Officer oversee implementation. Principals ensure that academy practice is consistent with this policy. Designated Safeguarding Leads manage safeguarding concerns; HR advises on employment matters; the Data Protection Officer advises on

personal data; Communications manages official publishing; and ICT manages account security, access, and relevant technical controls.

Managers must explain the standards relevant to each role, authorise official social media duties where appropriate and respond promptly to concerns. Everyone within scope must read and follow the policy, protect account credentials and information, maintain professional boundaries, and report safeguarding, security, data protection or conduct concerns without delay.

5. Core standards

Social media must be used lawfully, professionally, respectfully, and securely. The same standards of conduct apply online as offline. Individuals must not use social media to bully, harass, discriminate against, intimidate, threaten, defame, or deliberately humiliate another person, or to publish unlawful, abusive, or seriously offensive material. This includes conduct in private groups where it affects safeguarding, working relationships or the Trust.

No one may disclose personal, special category, criminal offence, safeguarding, confidential, commercially sensitive, or legally privileged information without authority and a lawful basis. Names, images, recordings, work samples, case details, screenshots, location information, or contextual clues must not be posted where they identify or may identify a pupil, parent, colleague, or other person unless publication has been properly authorised.

Personal opinions must not be represented as the Trust's position. A disclaimer may help clarify capacity but does not remove responsibility for a breach of confidentiality, safeguarding duties, professional standards, or law. Staff must not create unofficial accounts, pages, groups or campaigns using the Trust's or an academy's name, logo, or identity.

6. Official Trust social media

Only authorised staff may create, manage, or publish through an official Trust or academy account. New accounts, campaigns, and material changes of purpose require approval from the Communications lead and the relevant Principal or Trust Executive lead. Account ownership remains with the Trust, not the individual account administrator.

Official content must have a clear educational, operational or engagement purpose; be accurate, proportionate, inclusive and accessible; use an appropriate tone; and be checked before publication where the subject is sensitive, novel, or capable of significant impact. Political impartiality, safeguarding, copyright and advertising or endorsement risks must be considered. Comments and direct messages must be moderated under an approved approach, and contentious exchanges should be moved to an appropriate formal channel rather than argued publicly.

At least two authorised adults should normally have administrative access to each official account. Multi-factor authentication must be enabled where available. Credentials must be stored through an approved method and must not be shared through personal messages or reused across services. Access must be reviewed when duties change and removed promptly when an administrator leaves or no longer requires it.

7. Images, video, audio, and personal data

Before publishing personal information, photographs, video, audio, livestreams or pupil work, authorised staff must confirm the purpose, lawful basis, transparency information and any consent or preference arrangements required by the Trust. Consent will be used only where it is the appropriate lawful basis and must be capable of being withdrawn. A withdrawal will affect future use and will be acted upon where reasonably practicable, but it may not always remove material already lawfully distributed or reproduced by others.

Publishing must be limited to what is necessary. Staff should avoid unnecessary full names, precise locations, timetables, personal contact details, uniform or badge details, geolocation data and other information that could increase safeguarding risk. Personal devices and personal accounts must not be used to capture, store, edit or publish Trust content unless an exceptional arrangement has been expressly authorised and appropriate controls are in place.

Copyright and licence terms must be respected. Content created by others must not be copied merely because it is visible online. Where the Trust uses third-party material, the required permission, licence, or attribution must be obtained and recorded.

8. Staff personal use and professional boundaries

The Trust respects lawful personal use of social media. Staff are not required to identify their employer, connect with colleagues, or make personal accounts available to the Trust. They should nevertheless consider whether profile information, posts, comments, likes, shares, livestreams, group memberships, tags, or images could compromise safeguarding, confidentiality, professional boundaries, or public trust in their role.

Staff must not use personal accounts to conduct Trust business, communicate with pupils about Trust matters, receive work submissions, manage behaviour or safeguarding matters, or exchange personal contact details. Approved Trust accounts and systems must be used. Staff must not accept, initiate, or maintain personal social media connections with current pupils, except where the connection arises from a genuine family relationship and the member of staff has informed the Principal or DSL where a conflict or safeguarding risk may arise.

Requests or contact from pupils through a personal account should not be continued. The member of staff should preserve relevant evidence, avoid public engagement, block or restrict contact where appropriate and report the matter promptly to the DSL or Principal. Contact involving former pupils requires particular caution, especially where the former pupil is under 18, recently left the academy, remains vulnerable or an imbalance of power persists. Staff should seek advice before engaging where doubt exists.

Privacy settings should be reviewed, but they do not guarantee confidentiality. Staff should also manage tagging and location-sharing settings and ask friends or associates not to publish material that could create a safeguarding or professional concern. They must not attempt to gain access to another person’s restricted account, use a false identity, or ask a third party to obtain private content.

9. Messaging applications and online groups

Work-related communication with pupils, parents and carers must use approved Trust channels. Unauthorised WhatsApp, social media, or other personal-account groups must not be used for teaching, pastoral care, safeguarding, or routine Trust business. Where an approved messaging service is used, account ownership, membership, moderation, retention, and escalation arrangements must be clear.

Staff-only informal groups remain subject to confidentiality, dignity at work and professional conduct requirements where they concern Trust business or affect colleagues. Screenshots and forwarded content can widen an audience unexpectedly. Safeguarding information, health information, disciplinary or grievance material, pupil records and other sensitive matters must not be discussed in informal groups.

10. Safeguarding and online safety

Any social media content or contact that may indicate a child is at risk, involved in abuse, exploitation, harmful sexual behaviour, self-harm, extremism, criminal activity, or another safeguarding concern must be reported immediately through the Trust's safeguarding procedure. Staff must not investigate, promise confidentiality, confront an alleged perpetrator, or attempt to resolve the matter through social media.

Relevant evidence should be preserved in a safe and proportionate way without forwarding illegal or harmful material unnecessarily. Where imagery may constitute an indecent image of a child, staff must not view, copy, print, share or save it and must seek immediate advice from the DSL. Immediate danger or suspected crime should be escalated to the police or emergency services in accordance with safeguarding procedures.

Concerns about the online conduct of an adult working with children must be reported under the allegations and low-level concerns procedures. Concerns about the Headteacher or Principal must be reported to the designated senior Trust officer or Chair in accordance with the Child Protection and Safeguarding Policy.

11. Use during work and on Trust systems

Limited incidental personal use may be permitted during authorised breaks where it does not interfere with work, teaching, learning, safeguarding, network availability, security, or the rights of others and does not incur material cost. Permission may be restricted or withdrawn. Personal devices must use only the connection arrangements authorised by ICT and must not be used to bypass filtering, monitoring, or security controls.

Trust email addresses and contact details must not be used to register personal accounts. Trust information must not be copied to personal accounts, storage, or devices. Users must follow the ICT Acceptable Use Policy and report phishing, account compromise, suspicious links, accidental publication, or unauthorised access immediately.

12. Monitoring and access to information

The Trust may carry out lawful, fair, transparent, necessary, and proportionate filtering, logging, monitoring, retrieval, or investigation of activity on Trust systems, accounts, networks and devices for safeguarding, security, legal compliance, service management, and the investigation of suspected misconduct. The least intrusive reasonably effective method will be used, access will be restricted and relevant information will be provided through policies and privacy notices.

Monitoring of private or personal accounts will not be routine. The Trust may consider publicly available material; content voluntarily supplied to it or information lawfully obtained where there is a specific and legitimate concern. It will not normally require passwords, demand access to restricted profiles or use deception. A Data Protection Impact Assessment will be completed where monitoring is likely to result in a high risk to individuals. Covert monitoring will be exceptional, time-limited, specifically authorised, and subject to appropriate legal and data protection advice.

13. Recruitment and online searches

As part of safer recruitment due diligence, the Trust may conduct a proportionate online search of publicly available information about shortlisted candidates where this has been notified to them in advance. The purpose is to identify incidents or issues that are relevant to suitability to work with children and that may appropriately be explored at interview. The search is not a general investigation of a candidate's private life.

Searches must follow an approved process. Information must be relevant, accurate as far as reasonably possible and assessed in context. Protected characteristics, lawful trade union activity, and irrelevant personal opinions must not influence selection. Concerns will not be treated as established fact merely because they appear online; the candidate will ordinarily have a fair opportunity to respond. Records will be limited and retained in accordance with the recruitment privacy notice and retention schedule.

14. Concerns, complaints, and media enquiries

Concerns about inaccurate, abusive, defamatory, discriminatory, or confidential content relating to the Trust should be reported to a line manager, Principal, Communications lead, HR, DSL, or Data Protection Officer, according to the nature of the issue. Staff should not reply publicly on the Trust's behalf unless authorised. The Trust will decide whether to preserve evidence, request correction, or removal, use platform reporting tools, contact individuals, make a safeguarding or regulatory referral, or take legal advice.

Personal data breaches must be reported immediately under the Personal Data Breach Procedure. Security incidents must also be reported to ICT. Complaints from individuals about the use of their personal data will be handled under the Data Protection Policy and privacy complaints process. Nothing in this policy prevents a person from raising a safeguarding concern, reporting crime, obtaining independent advice, contacting a regulator, or making a protected disclosure under the Whistleblowing Policy.

15. Breaches and fair response

A breach may lead to restriction or removal of account or system access while the matter is assessed. Employees may be dealt with under the disciplinary procedure; other individuals may be dealt with under the procedure or contractual arrangements applicable to them. Serious cases may amount to gross misconduct, but no outcome is automatic. The Trust will establish the facts fairly, consider the individual's explanation and assess intent, context, reach, actual or potential harm, safeguarding risk, confidentiality, seniority, training, mitigation, consistency and any relevant disability or other circumstances.

The Trust may require the removal, correction, or preservation of content where this is lawful and proportionate. It cannot guarantee removal from third-party platforms or copies made by others. A safeguarding referral, data breach notification, report to a professional body, report to the police or legal action may be necessary in appropriate cases.

16. Records, training, and review

Records created under this policy will be accurate, relevant, secure, accessible only to those with a legitimate need and retained in accordance with the Trust's retention schedule. Official account content and direct messages that form part of Trust business may be official records and must not be deleted merely to avoid disclosure or scrutiny.

The Trust will provide proportionate induction and refresher information on professional boundaries, safeguarding, data protection, security, official account management, and incident reporting. Staff with publishing or moderation responsibilities will receive role-specific guidance.

This policy will be reviewed annually and sooner were legislation, statutory guidance, technology, platforms, risk, or Trust practice changes materially. Amendments will be approved through the Trust's governance arrangements and communicated to those affected.

Appendix 1: Quick response guide

Issue	Immediate response
A pupil contacts a personal account	Do not continue the exchange. Preserve relevant evidence, restrict or block contact where appropriate and report promptly to the DSL or Principal.
Possible safeguarding content	Follow the safeguarding procedure immediately. Do not investigate or circulate harmful material.
Account compromise or suspicious link	Stop using the account if needed, contact ICT immediately, change credentials through an approved route and preserve relevant information.
Personal data posted in error	Remove access where safe to do so and report immediately under the personal data breach procedure. Do not rely on deletion alone.
Abusive or inaccurate public post	Do not argue publicly on the Trust's behalf. Preserve evidence and refer to Communications, HR, the Principal or DSL as appropriate.
Media enquiry or high-profile issue	Refer the enquiry to the authorised Communications lead or Trust Executive lead. Do not provide an informal statement.