# Social Media Policy

| | | |
|---|---|---|
| **Approved by:** | Board of Trustees | **Date:** 07/10/2025 |
| **Last reviewed:** | September 2025 | |
| **Next review due by:** | September 2026 | |
| **Monitoring & Review** | HR – Annually | |

## Contents

## 1 Introduction

Social media applications give employees of CORE Education Trust and its schools opportunities to understand, engage, and communicate with audiences in a new way and acknowledge that new media has become a regular part of everyday life. The Trust understands the importance of using these technologies and services effectively and flexibly to instantly share the good news, and best practice and to build relationships, whilst maintaining a balance between our duties to our service users and partners, our legal responsibilities, and our reputation.

We recognise that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of platforms, such as Facebook, Twitter, WhatsApp, LinkedIn, Wikipedia, Instagram, Google+, Whisper, Tumblr, Vine, Instagram and all other social networking sites, internet postings, and blogs, etc. (collectively referred to as 'social media' in this policy). However, employees' use of social media can pose risks to our ability to safeguard children and young people, protect confidential information, and reputation, and can jeopardise our compliance with legal obligations.

Employees using social media are also potentially at risk of others misunderstanding the intent behind online communications or blurring professional boundaries between children and young people and their parents or carers. This policy, therefore, sets out the Trust's expectations regarding the use of social media.

To minimise these risks, to avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate business purposes and that the use of personal devices does not have an adversary impact on our business we expect employees to adhere to this policy.

## 2 Scope and purpose

2.1 this policy aims to ensure:

- That the reputation of the Trust and its schools is promoted correctly and positively and that both are not exposed to negative attention, legal or governance risks.
- Employees and students are protected.

2.2 The policy applies to the use of all social media whether during office hours or otherwise. The policy applies regardless of whether the social media is accessed using Trust ICT facilities and equipment or equipment belonging to members of staff.

2.3 This policy covers all employees working at all levels and grades. It also applies to consultants, contractors, casual and agency staff, and volunteers (collectively referred to as staff in this policy). Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

2.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.

## 3 Personnel responsible for implementing the policy

3.1 The Board of Trustees has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for its operation to the Headteacher within each school. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risk lies with the Board of Trustees who will review this policy to ensure that it meets legal requirements and reflects best practice.

3.2 All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understands the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

3.3 All staff are responsible for the success of this policy and should ensure that they take time to read and understand it. Any misuse of social media should be reported to the Headteacher and any questions regarding content or application of this policy should be directed to the Headteacher.

## 4 Compliance with related policies and agreements

4.1 Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- breach our ICT user policy;
- breach our obligations concerning the rules of relevant regulatory bodies;
- breach any obligations they may have relating to confidentiality;
- breach our Disciplinary Rules;
- defame or disparage the Trust or its affiliates, governors, students, parents and carers, staff, business partners, suppliers, vendors, or other stakeholders;
- harass or bully other staff in any way or breach our Anti-harassment and bullying policy;

- unlawfully discriminate against other staff or third parties or breach our Equal Opportunities Policy;

- breach our Data Protection Policy (for example, never disclose personal information about a colleague online);

- breach any other laws or ethical standards (for example, never use social media falsely or misleadingly, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive or negative, can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Staff may be required to remove social media postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## 5 Social Media for Official Trust Use

All proposals for using social media as part of the Trust whether hosted by the Trust or by a third party, must be approved by the Headteacher. This includes, but is not limited to, public-facing applications, such as open discussion forums and internally facing uses, such as project blogs regardless of whether they are hosted on the Trust/school network or not.

The Headteacher may require the employee to undergo training before they do so and impose certain requirements and restrictions about the employee's activities.

If the employee is contacted for comments about the Trust for publication anywhere (print or online), including any social media outlet, they must direct the inquiry to the Headteacher and must not respond without written approval.

## 6 Responsible use of social media

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely in order to protect staff and the Trust.

Employees' use of social media can pose risks to our ability to safeguard children and young people, protect our confidential information and reputation, and can jeopardise our compliance with our legal obligations. This could also be the case during off-duty time.

Safeguarding children and young people:

a) You should not communicate with students over social network sites. You must block unwanted communications from students.

b) You should never knowingly communicate with students in these forums or via a personal email account or using your school e-mail account where the communication is non-school related.

c) You should not interact with any ex-student of the Trust who is under 18 on such sites.

d) Communication with students should only be conducted through our usual channels. This communication should only ever be related to our business.

Protecting our business reputation:

Staff must not post disparaging or defamatory statements about:

a) our Trust;

b) our students or their parents or carers;

c) our governors or staff;

d) suppliers and vendors; and

e) other affiliates and stakeholders,

but staff should also avoid social media communications that might be misconstrued in a way that could damage our Trust's reputation, even indirectly.

In social media postings, staff should make it clear that they are speaking on their own behalf. Write in the first person and use a personal e-mail address when communicating via social media.

Staff are personally responsible for what they communicate on social media. Remember that what you publish might be available to be read by the masses (including the Trust itself, future employers, and social acquaintances) for a long time. Keep this in mind before you post content.

If you disclose your affiliation as an employee of our Trust, you must also state that your views do not represent those of your employer. For example, you could state, "The views in this posting do not represent the views of my employer". You should also ensure that your profile and any content you post are consistent with the professional image you present to students and colleagues.

Avoid posting comments about sensitive Trust-related topics, such as our performance. Even if you make it clear that your views on such topics do not represent those of the Trust, your comments could still damage our reputation.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with the Head Teacher/Line Manager/Director of Business and Operations.

If you see content in social media that disparages or reflects poorly on our Trust or our stakeholders, you should print out the content and contact the Headteacher/Line Manager/Director of Business and Operations. All staff are responsible for protecting our Trust's reputation.

## 7 Respecting Intellectual Property and Confidential Information

Staff should not do anything to jeopardise confidential information and intellectual property using social media.

Staff should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the Trust, as well as the individual author.

Do not use our logos, brand names, slogans, or other trademarks, or post any of our confidential or proprietary information without prior written permission.

To protect yourself and the Trust against liability for copyright infringement, where appropriate, reference sources of particular information posted or uploaded must be cited accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher before making the communication.

Any business contacts made during your employment are regarded as our confidential information and, as such, you will be required to delete all such details from your social networking accounts, such as Facebook accounts or LinkedIn accounts, on termination of employment.

Respecting colleagues, students, parents and carers, governors, and other stakeholders:

a) Do not post anything that your colleagues or our students, parents and carers, governors, and other stakeholders would find offensive, including discriminatory comments, insults, or obscenity.

b) Do not post anything related to your colleagues or our customers, clients, business partners, suppliers, vendors, or other stakeholders without their written permission.

Unless it is about finding candidates (for example, if an individual has put his/her details on social media websites to attract prospective employers), the School /

Academy / Trust may conduct searches, either themselves or through a third party, on social media only when these are directly relevant to the applicant's skills or claims that he/she has made in the recruitment process. For instance:

a) a prospective employee might claim that he/she has used social media in his/her previous job (for example, as a publicity tool); or

b) a prospective employee's social media use may be directly relevant to a claim made in his/her application (for example, if he/she runs a blog based around a hobby mentioned in his/her CV or a skill in which he/she claims to be proficient).

There should be no systematic or routine checking of prospective employees' online social media activities, as conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision. This is in line with the Trust's Equal Opportunities policy.

## 8 Monitoring of ICT Facilities

The contents of our IT resources and communications systems, held in whatever media, including information and data held on computer systems, hand-held devices, tablets, or other portable or electronic devices and telephones, relating both to the Employer's education provision or any students, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

We may monitor, intercept and review, without further notice, staff activities using our ICT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules and regulatory duties are being compiled with and for legitimate business purposes and you consent to such monitoring by your acknowledgment of this policy and your use of such resources and systems.

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

We will comply with the requirements of Data Protection Legislation (being (i) the General Data Protection Regulation ((EU) 2016/679) (unless and until the GDPR is no longer directly applicable in the UK) and any national implementing laws,

regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998, including the Data Protection Act 2018), in the monitoring of our IT resources and communication systems Monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.

In line with the requirements of Data Protection Legislation, we may store copies of such data or communications for some time after they are created and may delete such copies from time to time without notice. Records will be kept by our Staff Privacy Notice, and our Retention and Destruction Policy.

Do not use our IT resources and communications systems for any matter that you wish to be kept private or confidential from the Trust.

## 9 Trust/School Email Address for personal use

Staff must only use their work email address for official Trust purposes. If staff are found to be using their work email address for personal use, they may face disciplinary action.

## 10 Using Social Media for Personal Use

Personal use of social media is never permitted during working hours or using our computers, networks and other IT resources and communications systems, unless it has been authorised by the Headteacher, a member of the Trust Executive, or a delegated person of authority. Staff should ensure any personal accounts are 'closed' or 'private' and that they monitor requests to access and report any unusual activity or persistent requests asap to their line manager in the first instance.

## 11 Breach of this Policy

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used to commit the breach. Any member of staff suspected of committing a breach of this policy will be required to cooperate with our investigation, which may involve handing over relevant passwords and login details.

Staff may be required to remove any social media content that the Trust considers to constitute a breach of this policy. Failure to comply with such a request may, result in disciplinary action.