



EVERYONE MATTERS
SCHOOLS TRUST

Social Media Policy

Everyone Matters Schools Trust Central Policy



Policy Owner	Trustees and CEO
Scope of the Policy	This policy applies to all of the schools in the EMST community
Last reviewed by trustees	June 2025
Next review due	June 2027
Summary of key changes	Responsible person is identified as CEO/ Principal or Headteachers in Trust schools.
Committee Responsible	Trustees

HEAD OFFICE
HIGHER LANE RAINFORD ST HELENS
MERSEYSIDE WA11 8NY
COMPANY NO: 10455406 10455406

1 SCOPE AND PURPOSE

- 1.1 In this policy 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks or platforms, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking services and user rating services.
- 1.2 Social media is an ever-growing phenomenon with an increasing importance to the Trust and schools reputation. However, there are risks associated with social media use and the aim of this policy is to minimise those risks to our Trust, our schools and their reputation.
- 1.3 To minimise these risks and to ensure that the Trust's IT resources and communications systems are used only for appropriate purposes, the Trust expects staff to adhere to this policy.
- 1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.
- 1.5 This policy is in place to minimise the risks to the Trust through the use of all forms of social media, including social and business networking sites (e.g. Facebook, LinkedIn, Twitter), instant messaging services (e.g. WhatsApp, Snapchat), video and image sharing sites (e.g. YouTube, Tik Tok, Instagram, Pinterest and Flickr) as well as Wikipedia and more traditional personal blogs and topic based forums use of social media.
- 1.6 It applies to the use of social media for both professional and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using the Trust's IT facilities and equipment or equipment belonging to members of staff.
- 1.7 Breach of this policy may result in disciplinary action up to and including dismissal.
- 1.8 Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the Trust's equipment or facilities are used for the purpose of committing the breach.
- 1.9 Any member of staff suspected of committing a breach of this policy will be required to co-operate with any investigation that may follow, which may involve handing over relevant passwords and login details.
- 1.10 Staff will be required to remove internet 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.

2 WHO IS COVERED BY THIS POLICY?

- 2.1 This policy covers all individuals working at all levels and grades throughout the Trust, including trustees, governors, consultants, contractors, trainees, part time and fixed term employees, casual staff, agency staff and volunteers (collectively referred to as staff in this policy).

2.2 Third parties who have access to the Trust's electronic communication systems and equipment are also required to comply with policy.

(1) **Who is responsible for the policy?**

2.3 The Trust Board has overall responsibility for the effective operation of this policy. The Trust Board has delegated day-to-day responsibility for operating this policy and ensuring its maintenance and review to the CEO/Principal and Headteachers of the Trust schools.

2.4 The Senior Leadership team and all other managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Training will, if required, be provided to facilitate this.

2.5 All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Principal.

2.6 Questions regarding the content or application of this policy should be directed to the Principal.

3 **COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS**

3.1 Social media should never be used in a way that breaches any the other policies of the Trust. If an internet post would breach any of the Trust's policies in another forum, it will also breach them in an online forum. Staff are prohibited from using social media to:

3.1.1 breach any obligations the Trust has in relation to the duty of confidentiality to its staff, trustees and pupils, both past and present;

3.1.2 breach Trust's disciplinary policy;

3.1.3 defame or disparage the Trust, its staff, trustees, pupils and third parties connected with the Trust, for example pupils' parents;

3.1.4 post commentary, content or images that are extremist, incitement to violence, sexist, racist, Islamophobic, anti-Semitic, homophobic, proprietary, harassing, libellous or that can otherwise create a hostile working environment;

3.1.5 breach the Trust's IT and communications systems policy;

3.1.6 breach the Trust's anti-harassment and bullying policy;

3.1.7 breach the Trust's equal opportunities policy;

3.1.8 breach the Trust's data protection policy;

3.1.9 breach the Trust's obligations for Keeping Children Safe in Education;

3.1.10 breach the Trust's obligations with respect to the rules of relevant regulatory bodies;

- 3.1.11 breach any other laws or ethical standard.
- 3.2 In addition, staff should not make postings in any forums where prohibited social media postings are made by others. If such a posting is made, staff are expected to desist from engaging in such forums in the future.
- 3.3 Staff should not promote social media sites of individuals or groups, or join online forums and groups with individuals, that are known to have views which may be considered extremist in nature. If staff are in doubt, they should speak to a member of the Senior Leadership Team of the Trust or their school.
- 3.4 Staff should never provide references for other individuals on social or professional networking sites. Such references, whether positive or negative, can be attributed to the Trust and create legal liability for the Trust accordingly and the individual providing the reference.
- 3.5 If staff breach any of the above policies they will be subject to disciplinary action up to and including termination of employment.

4 GENERAL PRINCIPLES

- 4.1 The following general principles apply throughout this policy:
 - 4.1.1 Staff members will be assumed to be personally responsible for anything posted on any social media account associated with them. Therefore, the Trust's recommends that staff do not share their log-in details with anyone else, or leave their phone or other personal devices unattended;
 - 4.1.2 If a social media site records the time and/or date of a posting made by a member of staff, this will be deemed to be accurate unless the contrary is proven;
 - 4.1.3 Always remember that anything posted online is never completely private. In particular, staff should not assume that they have any entitlement to privacy in respect of anything they post on a social media site which can be freely viewed by pupils, parents, members of the public, other staff members or third parties we deal with; and
 - 4.1.4 If staff post anything on a social media site which is in breach of this policy, or of any of the Trust's other policies or procedures, they should be aware that whilst they should delete the posting promptly, doing so will not exonerate them from the breach and they may still be liable to disciplinary action.

5 PERSONAL USE OF SOCIAL MEDIA

- 5.1 Staff are strictly forbidden from accessing or using social media for personal purposes during working hours, whether by means of Trust's computer network or communications systems, or by means of personal devices (e.g. iPads, tablets or mobile telephones). Any personal use must be limited to before or after work, and during break and lunch times.

- 5.2 Staff should at all times be aware that if they access social media for personal use, whether during working hours, on Trust premises or outside of work, they must comply with this policy at all times including the social media guidelines for responsible usage below.

6 EDUCATIONAL AND/OR BUSINESS USE OF SOCIAL MEDIA

- 6.1 Some staff members may be permitted / required to post content or comments in a social media environment in order to build the social media profile of the Trust or School. [Likewise, some staff members may find it useful to use business-networking sites such as LinkedIn to maintain communication with existing business contacts and make new business connections.] If a member of staff is using social media for educational and/or business purposes, the following additional rules will apply:
- 6.1.1 Staff members must have prior approval from their manager before engaging in the business use of social media during working hours;
- 6.1.2 Staff remain at all times subject to the remainder of this policy, in particular the general principles set out above, and must follow the social media guidelines for responsible use set out below;
- 6.1.3 If required to do so, staff must use any social media accounts, profiles and pages set up and paid for by the Trust for educational and/or business purposes. Where such accounts exist, staff are forbidden from using personal accounts for educational and/or business purposes;
- 6.1.4 Staff must not share the log-in details of any social media account used for educational and/or business purposes with anyone else without prior written approval from their manager;
- 6.1.5 Staff must use the Trust computer network or communication system to access and use social media for educational and/or business purposes **and any photos may only be taken using Trust cameras or devices**. Staff must not use a personal device (e.g. an iPad, tablet or mobile telephone) unless expressly permitted to do so by their manager; If a personal device is used to take pictures for the use on trust/school social media sites the images must be deleted **from the device immediately** after they have been used for the agreed purpose **or uploaded to a device belonging to the school**.
- 6.1.6 Staff must ensure that individuals have given prior consent before posting their personal information. Ensure that specific permission from students' parents/carers has been sought before their information is used on social media.
- 6.1.7 Staff must ensure that there is no identifying information relating to a student/students' in any post, for example any certificates or pieces of work in photos should be without names or have the names obscured. Additional consent should be sought to include any names when posting on social media.
- 6.1.8 Staff may be required to undergo training on the educational and/or business use of social media;

- 6.1.9 The Trust may impose certain requirements and restrictions regarding staff activities (including the nature of the material posted, the sites staff are permitted to access during working hours and the amount of working time staff are allowed to spend on social media activities); and
- 6.1.10 If staff are contacted for comments about the organisation for publication anywhere, including in any social media outlet, they must not respond without written approval. Please direct the enquiry to the Principal.

7 GUIDELINES FOR RESPONSIBLE USE OF SOCIAL MEDIA

- 7.1 The following sections of the policy provide staff with common-sense rules, guidelines and recommendations for using social media responsibly and safely.
- 7.2 Staff should not use a work email address to sign up to any social media or associate themselves with the Trust on their profile or in any postings.
- 7.3 Staff **must not** have any direct contact (or be 'friends') with pupils on any social media platform unless they are a member of their immediate family (if a member of staff is found to be in breach of this requirement it will be considered an act of potential gross misconduct and dealt with under the Trust's Disciplinary Policy).
- 7.4 Staff are **strongly advised** not to have any direct contact (or be 'friends') with parents on any social media platform unless they are a member of their immediate family.
- 7.5 Protecting the Trust's reputation:
- 7.5.1 Staff must not post disparaging or defamatory statement about:
- 7.5.1.1 the Trust as an organisation;
- 7.5.1.2 **current, past or prospective** members of staff, trustees, trainees or pupils;
- 7.5.1.3 **third parties connected with the Trust, e.g. parents, carers or families of pupils, suppliers, service providers or other affiliates and stakeholders.**
- 7.6 Staff should also avoid social media communications that might be misconstrued in a way that could damage the Trust's reputation, even indirectly.
- 7.7 Staff should make it clear in social media postings that they are speaking on their own behalf, and not on behalf of the Trust, its officers or employees. A way to achieve this would be writing in the "first person".
- 7.8 If a member of staff **directly or indirectly** discloses their affiliation with the Trust they should state that their views do not represent those of their employer. For example, they could state, "the views in this posting do not represent the views of my employer".
- 7.9 Staff are personally responsible for what they communicate in social media.
- 7.10 Staff should ensure that **their profile and** the content of their postings are consistent with professional image as a member of staff of the Trust.

- 7.11 Staff must avoid posting comments about confidential or sensitive Trust related topics. Even if staff make it clear that their views on such topics do not represent those of the Trust, such comments could still damage the Trust's reputation and incur potential liability.
- 7.12 If staff are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they discuss it with the Principal/Headteacher
- 7.13 If a member of staff sees content in social media that disparages or reflects poorly on the Trust including its staff, pupils, parents, service providers, trustees or stakeholders, they should contact the Principal/ Headteacher or CEO. All staff are responsible for protecting the reputation of the Trust.
- 7.14 Staff should not do anything to jeopardise confidential information and intellectual property of the Trust its staff or pupils (past or present) through use of social media.
- 7.15 Staff should avoid misappropriating or infringing the intellectual property of other schools, organisations, companies and individuals as this may create liability for both themselves and the Trust.
- 7.16 Staff should be respectful to others when making a statement on social media and should not post anything that colleagues and pupils (prospective, past and/or current) or third parties would find offensive, including discriminatory comments, insults or obscenity.
- 7.17 Staff **must not** make or posts or comments which may be deemed to incite racial or religious hatred or which may be in breach of any other law;
- 7.18 Staff should not post anything related to their colleagues or pupils without their or their parents written permission and consent (including consent for use of photographs/videos).
- 7.19 Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- 7.20 Staff must not take any photos or posts from social media that belong to the Trust for their own personal use.
- 7.21 Staff must not use the Trust's logos, brand names, slogans or other trademarks, or post any of the Trust's confidential or proprietary information without express prior written permission from the Principal/Headteacher or CEO.
- 7.22 To protect yourself and the Trust against liability for copyright infringement staff should where appropriate reference sources of particular information posted or uploaded and cite them accurately.

8 MONITORING

- 8.1 The Trust reserves 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, to ensure that our rules are being

complied with and for legitimate business purposes and staff consent to such monitoring by their use of such resources and systems.

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

8.3 The Trust may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

8.4 The contents of our IT resources and communications systems are the Trusts property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message or any other kind of information or communications transmitted to, received, printed from stored or recorded on the Trust's electronic information and communications systems.

8.5 All Staff are advised not to use the Trust's IT resources and communications systems for any matter that they wish to be kept private or confidential from the Trust.

9 **RECRUITMENT**

9.1 The Trust's may use internet searches to perform due diligence on candidates in the course of recruitment. Where the Trust's does this, it will act in accordance with its data protection and equal opportunities obligations.