East Midlands Academy Trust

Social Media Policy 2022/2023

'Every child deserves to be the best they can be'

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V2	**Filename:** EMAT Social Media Policy.doc
Approved: June 2022	**Next Review: June 2023** This policy will be reviewed annually by the Trust Board (FHRE committee)
Owner: EMAT Board of Trustees Head of Shared Services and HR Team	

Policy type:	
Statutory	Replaces Academy's current policy

Referenced Policies / Proceedure
ICT Acceptable Usage Policy Investigation procedure Online safety Code of conduct Disciplinary policy

Revision History

RevisionDate	Revisor	Description of Revision
June 2022	M Juan	Policy review – No Changes
July 2021 – V2	M Juan	Policy review – No Changes
July 2020 – v1	M Juan	New EMAT Social Media Policy

EMAT Social Media Policy

1. Introduction

The principles set out in this policy are designed to ensure that all staff, trustees, governors and volunteers have a clear framework and explicit details on the appropriate and safe use social media and definition of unacceptable behaviours and activity on social media.

The internet is fast moving technology and it is impossible to cover all circumstances or emerging media. Therefore, the principles set out in this policy must be followed closely, irrespective of the medium or platform.

Whilst this policy is not intended to prevent employees from using social media sites, it does aim to make employees aware of the risks they could face whilst doing so and highlight what is deemed to be unacceptable when sharing information about their professional and/or personal life.

This policy has been produced to deliver the following outcomes:

- Ensure staff, trustees, governors and volunteers are aware of the Trust's expectations when using social media, protecting them from accidently undertaking unacceptable behaviour.
- Minimise the reputational, legal and governance risks to the Trust and its staff, trustees, governors and volunteers, arising from use of social media by staff in both personal and professional capacities.
- To enable the safe use of social media for the purposes of communication and engagement.
- To ensure a consistent approach is applied across the Trust.
- To identify responsibilities of the Trust its staff, trustees, governors and volunteers in line with the following policies:
    - Safeguarding Policy
    - GDPR
    - Dignity at Work
    - Professional Standards Legal implications
    - Online Safety
    - Code of conduct
    - Disciplinary Policy

It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

2. Responsibility

It is the responsibility of all staff, trustees, governors and volunteers within East Midland Academy Trust (**EMAT**) to read and understand and comply with this policy. This policy is reviewed on an annual basis but is liable for amendments more frequently to comply with changes in governance or to address technology trends.

Staff, trustees, governors and volunteers must be aware of and act in accordance with their duties under the DfE statutory guidance Keeping Children Safe in Education 2020 this policy relates to:

- Their own online activity.
- The online activity of students and other colleagues.
- Information of which they become aware on-line.

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with members of staff as part of staff induction and CPD days. Safe and professional behavior will be outlined for all staff as part of our Employee Code of Conduct and as part of our Acceptable Use policy on an annual basis.

Staff, trustees, governors and volunteers must be conscious of the need to keep their personal and professional lives separate.

All staff, trustees, governors and volunteers must be aware that as soon as a post is made online, it is no longer within the private sphere or in the control of the original poster.

All staff, trustees, governors and volunteers should be aware that once something is posted online is it nearly impossible to permanently erase, screen shots can be made and comments can be forwarded or shared.

Staff, trustees, governors and volunteers should be aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of:

- Libel
- Copyright
- Discrimination
- Contract
- Human Rights
- Protection from harassment
- Criminal Justice
- GDPR (Data Protection)

If a member of staff, a governor or volunteer becomes aware of any breach of this social media policy, it must be reported promptly to the head teacher or member of the Trust's executive team and if required also the designated safeguarding lead whether carried out by parents/guardians or staff/governors.

3. Scope

This policy equally applies to all staff, trustees, governors and volunteers and any other individuals who work for or provide services on behalf of the Trust.

This policy covers personal use of social media as well as the use of social media for official Trust purposes by appointed staff, trustees, governors and volunteers.

The policy applies to personal media platforms such as social and networking sites (e.g. Facebook, Twitter, Instagram, LinkedIn), blogs, chatrooms, forums, podcasts, open access, online encyclopaedias such as Wikipedia and content sharing sites (flickr and YouTube) and online message boards/forums and comments under news items and other articles. This list is not exhaustive and new on-line platforms are to be considered automatically covered.

4. Policy

The policy has been split in the following sections

- Communications
- Personal Use of Social Media
- Information
- Cyber Bullying and Cyber Harassment
- Trust Related Social Media Accounts and Activity

4.1 Communications

In all communications from Trust staff, trustees, governors and volunteers must:

- Be conscious at all times of the need to keep personal and professional lives separate. Staff, trustees, governors and volunteers should not put themselves in a position where there is a conflict between their work and personal interests.
- Not engage in activities involving social media which may bring the Trust into disrepute. E.g by making derogatory or defamatory comments, either directly or indirectly, about the school, colleagues, individuals, pupils or parents etc. that could negatively impact on the schools reputation or cause embarrassment. This includes posting images or links to inappropriate content or using inappropriate language.
- Not represent their personal views as those of the Trust on any social medium.
- Not breach confidentiality. E.g. revealing confidential information owned by the school relating to its activities, finances, employees or pupils.
- Not undertake any behaviour which may be considered discriminatory, or as bullying and/or harassment of any individual. E.g. making offensive or derogatory comments (either directly or indirectly) relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully (“Cyberbullying”) another individual; or posting images that are discriminatory or offensive or linking to such content.
- Follow safeguarding principles.
- Be open, honest, ethical, and professional.

4.2 Personal use of Social Media

The Trust respects the privacy of its staff, trustees, governors and volunteers. However, postings made on personal accounts may attain a wide readership and will therefore be considered public rather than private. Publicly accessible postings may be investigated if there is a suspected breach of this or related policies or could bring the ethos of the trust in disrepute.

Never create a personal social media account in a way that could be confused as an official Trust account.

When a public post is reported concerning non-employee members of the school community, this will be investigated and responded to by the Trust. Further action may be taken to assist with the prosecution of the offenders.

Staff, trustees, governors and volunteers are not permitted to react or respond to posts by third parties, even if it is in defense of the Trust. Advice should always be sought from the PR and Communications Manager who manages the Trust's social media channels.

Staff, trustees, governors and volunteers are strongly encouraged not to identify themselves as members of the Trust community in their personal social media platforms with the exception of professional network forums such as LinkedIn or professional discussion board/forums. This is to prevent information on these sites from being linked with the Trust and to safeguard the privacy of staff, governors and volunteers.

Staff, trustees, governors and volunteers should not have contact through any social medium with any student from within the Trust or any other school.

Staff, trustees, governors and volunteers are advised not to communicate on social media platforms with ex-students except via professional networking sites for professional reasons.

Staff, trustees, governors and volunteers should decline 'friend requests' from students they receive in their personal social media accounts.

Staff, trustees, governors and volunteers should also carefully select their social media profile picture as it is an extension to their professional image online.

Staff, trustees, governors and volunteers are strongly advised to ensure that they set up and regularly review the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff, trustees, governors and volunteers should keep their passwords confidential, change them often and be careful what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

Personal social media should not be used for work related communication. Communication should be through the Trust's ICT Infrastructure and services including but not limited to work email, MS Teams, Trust supplied mobile phones using text messaging or call and communication should only be carried out using contact details held by the Trust.

Staff are permitted and encouraged to follow official Trust activity and accounts on social media and share as they wish. If you are unsure, please contact the PR and Communications Manager.

Members of staff who follow/and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries. If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- always be professional and aware they are an ambassador for the setting;
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared;
- always act within the legal frameworks, they would adhere to within the workplace;
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so;
- inform their line manager, the DSL or the Headteacher of any concerns, such as criticism, inappropriate content or contact from students.

4.3 Information

Staff, governors and volunteers whom have access to as part of their employment personal or sensitive data, organisationally sensitive information or information relating to follow staff members, students and their family members or any other parties linked to the trust, must never disclose or share such information on personal social media platforms.

Photographs, videos or any of images of pupils or students should not be published on personal social media platforms without prior permission of parents/carers and the Trust. Permission should be gained through existing school procedures. School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media unless pre-approved by the Trust's executive team.

4.4 Cyber Bullying and Cyber Harassment

Staff must never engage with cyberbullying incidents and should immediately report incidents to the headteacher or a member of the Trust's executive team and if required the designated safeguarding lead

A person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed online in any format still fits the criteria of cyber bullying/harassment. The Trust will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the Trust or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work.

4.5 Trust Related Social Media Accounts and Activity

If a member of staff, a governor or volunteer identifies the need to create a social media account linked to the Trust (i.e. department, activity group etc.) A written request must be submitted to the PR and Communication Manager for consideration. The request should detail what the account will be used for and who by. If approved the social media account will be created by the PR and Communication Manager **not** the requestor. The relevant account details will then be shared to approved staff, governors or volunteers by the PR and Communication Manager who retains overall control of the account and a record of individuals who have been issued with the details.

Staff, governors and volunteers are not permitted to change or amend log on credentials to Trust owned Social media accounts this can only be done by the PR and Communication Manager.

The PR and Communications Manager reserves the right delete or amend content posted or terminate the account if deemed inappropriate

Under no circumstances should social media account passwords be shared with any other party by anyone other than the PR and Communications Manager.

If staff, trustees, governor or volunteers are participating in online social media activity as part of their professional capacity to the Trust, they will:

- always be professional and aware they are an ambassador for the setting;
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared;
- always act within the legal frameworks, they would adhere to within the workplace;
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so;
- inform their line manager, the DSL or the Headteacher of any concerns, such as criticism, inappropriate content or contact from students.

5. Exceptions

In cases where staff, trustees or governors are also parents/guardians connected to the school, they are advised to use professional judgment (in reference to child protection and safeguarding policies) when communicating with other children or young people also connected to the school community. This relationship should stand up to scrutiny from a professional perspective and should be appropriate. If a concern of safeguarding arises, this should be reported to the designated safeguarding lead

If staff, trustees, governors or volunteers are using Professional Social media services such as LinkedIn or other professional forums and discussion groups to interact with peers and part of continuous personal development and for personal and professional betterment it is permitted to associate yourself with the Trust, however it must be clear that you do not speak on behalf of the Trust unless this has been explicitly granted by the Trust's executive team, all other section of this policy remain applicable. If you are unsure contact the Trust's PR and Communications Manager

If staff have been granted access to accounts used to access Trust social media accounts and their job description indicates that they are permitted comment or post on behalf of the Trust then they will be exempt from certain sections of 4.3 as long as they are using the Trust's official account and not personal account. This exemption also applies for members of the Trust's executive team. If you feel that you should also be included in this exemption, please confirm with the PR and Communications Manager

6. Consequences of Breach of Policy

In the event of a breach of this Social Media Policy User the Trust may in its sole discretion:

- The Trust may take disciplinary action up to and termination of employment
- Disclose information to law enforcement agencies and assist with the prosecution of the offenders
- The Trust may take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith
- restrict or terminate a User's right to use the Trust ICT Infrastructure;
- withdraw or remove any material uploaded by that User in contravention of this Policy;

7. Monitoring

All Trust ICT systems may be monitored in accordance with the ICT Acceptable Use Policy, so personal privacy cannot be assumed when using school hardware, software or services. The Trust can monitor the usage of its own Infrastructure and services (internet access, email, teams, Wi-Fi etc.) as well as activity on end user compute (Tablets, Laptops, Desktop computer, mobile phones etc.) without prior notification or authorisation from Users when justifiable concerns have been raised. This will be in line with the Trust's Investigation procedure which available from the Trust's HR team on request

8. Definitions

ICT Infrastructure – all computing, telecommunication, software, services and networking facilities provided by the Trust either onsite at any of its Academies or related premises or remotely, with reference to all computing devices, either personal or Trust owned, connected to systems and services supplied by the Trust.

Staff – Those working for the Trust on a full time, part time or flex time basis, apprentices, agency workers and contractors.

Users - any person granted authorisation to use any computer or device on the Trust ICT Infrastructure. This includes (but is not limited to) staff, students, visitors, customers (tenants or using site facilities), temporary workers, contractors, vendors, volunteers and sub-contractors authorised to access the network locally or remotely, for any reason, including email and Internet or intranet web browsing

Public – This refer to those outside of the immediate Trust community of Staff and students and includes (but not exclusively) parents/carers and ex-pupils.

The Trust - refers to the East Midlands Academy Trust, Central Services and all Academies and sites associated with it.