Social Media Policy

*For the purposes of this policy, '**the Trust**' refers to **The Trust and all schools** within the Trust*

Monitoring and review	
Author	Helen Reeves
Approver	Trustees
Owner	Helen Reeves, Director of Human Resources
Most recent review date:	September 2025
Date of next review	**September 2026**
Review frequency:	Annual
Category of policy	Statutory
Who has been consulted	
Adapt or Adopt	Adapt

Document version control

Version	Changes made	Amended By	Date
1	Initial Issue		
1.1	Adapted by MGS	WG	Oct 2026

Contents

1. **Context** 3

2. **Purpose of This Policy** 3

3. **Who is Covered by This Policy?** 4

4. **Scope and Purpose of This Policy** 4

5. **Personnel Responsible for Implementing This Policy** 4

6. **Compliance with Related Policies and Agreements** 5

7. **Personal Use of Social Media** 5

8. **Monitoring** 6

9. **Educational and Extra-Curricular Use of Social Media** 6

10. **Recruitment** 7

12. **Protecting our Business Reputation:** 7

13. **Monitoring and Review of This Policy** 8

Appendix A: Staff Protocol for the use of Social Media *10*

1. Context

This policy applies to all Trust staff regardless of their employment status. It is to be read in conjunction with the Trust's Acceptable Use Policy. This policy does not form part of the terms and conditions of an employee's employment with the Trust and is not intended to have contractual effect. However, it does set out the Trust's current practices and required standards of conduct. All staff are required to comply with its contents. Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the Trust's Disciplinary Policy and Procedure.

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

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.

2. Purpose of This Policy

The Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media such as Facebook, Twitter, LinkedIn, blogs, Instagram, TikTok, WhatsApp and Wikipedia. However, staff use of social media can pose risks to the Trust's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work-related purposes, all Trust staff are required to comply with the provisions in this policy.

Social media platforms allow us to build connections and to share ideas and content more broadly and quickly, and the Trust supports their use. However, improper use of social media may give rise to a breach of your contract and/or the Trusts policies, and/or the following:

- Bullying, harassment and unlawful discrimination.
- Defamation (i.e., damaging the good reputation of another person or organisation)
- Contempt of court (i.e., interfering with the administration of justice e.g., by revealing someone's identity that had been protected by the courts)
- Breach of data protection laws.
- Misuse of confidential information belonging to the Trust or to its students/staff/ parents/suppliers.

- Damage to reputation of the user or Trust or to its students/staff/parents/suppliers

3. Who is Covered by This Policy?

This policy covers all individuals working at all levels and grades within the Trust, including senior managers, officers, governors, trustees, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, 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.

4. Scope and Purpose of This Policy

This policy deals with the use of all forms of social media including Facebook, LinkedIn, Twitter, Wikipedia, Instagram, TikTok, WhatsApp and all other social networking sites and all other internet postings including blogs.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

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 the Trust's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

Staff may 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.

5. Personnel Responsible for Implementing This Policy

The Trustees have overall responsibility for the effective operation of this policy but have delegated day-to-day responsibility for its operation to the CEO and Headteachers.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the CEO in liaison with the IT Manager.

All senior Staff 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.

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 Headteacher or CEO in the first instance. Questions regarding the content or application of this policy should be directed by email to The Human Resources Director on office@aptmat.co.uk

6. Compliance with Related Policies and Agreements

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 Acceptable IT Use policy
- Breach our obligations with respect to the rules of relevant regulatory bodies
- Breach any obligations they may have relating to confidentiality
- Breach our Disciplinary Policy
- Defame or disparage the Trust, its staff, its pupils or parents, its affiliates, 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 Equality Information and Objectives Policy
- Breach our Data Protection policy (for example, never disclose personal information about a colleague, student, parent, or any other individual online)
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements) and
- Breach our obligations for Keeping Children Safe in Education.

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

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

7. Personal Use of Social Media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems.

Staff should not use a work email address to sign up to any social media. Staff personal social media pages should not make reference to their employment with the Trust (excluding social media pages specifically intended for business purposes such as LinkedIn).

Staff must not take photos or posts from social media that belong to the Trust for their own personal use.

8. Monitoring

The contents of our IT resources and communications systems are the Trust's 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 or printed from or stored or recorded on our electronic information and communications systems.

The Trust reserves the right to monitor, intercept and review, without further notice, Staff members 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. By your acknowledgement of this policy consent to such monitoring 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-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

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.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the Trust. All content on our systems is subject to access requests under the Freedom of Information Act.

9. Educational and Extra-Curricular Use of Social Media

If your duties require you to speak on behalf of the Trust in a social media environment, you must follow the protocol outlined below.

The Headteacher or CEO may require you to undergo training before you use social media on behalf of the Trust and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the Trust for publication anywhere, including in any social media outlet, you must direct the inquiry to the Headteacher or CEO and must not respond without advanced written approval.

As part of this role, you will be required to ensure individuals have given prior consent before posting their personal information. You will also need to monitor the messages/posts coming through. Subject Access Requests (SARs) can be made via social media platforms.

10. Recruitment

The Trust may use internet searches to perform pre-employment checks on candidates in the course of recruitment. This is after the shortlisting and interview stage in order to make a final decision on where to recruit, including criminal record information, references, and information regarding qualifications. Where the Trust does this, it will act in accordance with its data protection and equal opportunities obligations.

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

11. Responsible Use of Social Media

Photographs for use with social media:

Any photos for social media posts may only be taken using Trust cameras/devices or devices that have been approved in advance by the HR lead in the school or Trust. Where any device is used that does not belong to the Trust, all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the Trust.

Staff protocol for use of social media: (See Appendix A)

12. Protecting our Business Reputation:

Staff must not post disparaging or defamatory statements about:

- The Trust
- Current, past or prospective Staff as defined in this policy
- Current, past or prospective pupils
- Parents, carers or families of (iii)
- The Trust's suppliers and services providers and
- Other affiliates and stakeholders
- Current, past or prospective governors and trustees.

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

If Staff are using social media they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than Trust e-mail address when communicating via social media.

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

If Staff disclose directly or indirectly their affiliation to the Trust as a member of Staff whether past, current or prospective, they must also state 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 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.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with his/her Line Manager or Head of Department.

If a member of Staff sees content on social media that disparages or reflects poorly on the Trust including its Staff, pupils, parents, service providers, stakeholders, trustees or governors, they are required to report this in the first instance to the Headteacher or CEO without unreasonable delay. All staff are responsible for protecting the Trust's reputation.

Respecting intellectual property and confidential information:

Staff should not do anything to jeopardise Trust confidential information and intellectual property through the use of social media.

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

Staff must not use the Trust's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Headteacher or CEO.

To protect yourself and the Trust against liability for copyright infringement, the Staff member should, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders:

Staff must not post anything that their colleagues (past and/or current), pupils (prospective and/or current), parents, service provider, stakeholders or governors may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything relating to colleagues (past and/or current) or pupils, parents (prospective and/or current) service providers, stakeholders or governors without their advanced written permission.

13. Monitoring and Review of This Policy

The CEO shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Trustees have a responsibility for approving any amendments prior to implementation.

The CEO has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

If Staff have any questions about this policy or suggestions for additions that they would like to be considered on review, they may do so by emailing The Director of Human Resources on office@aptmat.co.uk in the first instance.

Appendix A: Staff Protocol for the use of Social Media

Whatever you write relating to your work or using work systems, whether via an email, on a web forum/extranet, by text or within a letter means that you are corresponding on behalf of the school and the school is considered to be the publisher.

Such correspondence can be produced as evidence in Court or at an employment tribunal or other recognised authority and can be disclosed under the GDPR or Freedom of Information Act.

If staff are writing about an individual it is likely to be considered personal information under the General Data Protection Regulation (GDPR) if contains identification details such as name, age, gender, address and phone numbers, bank account details or nationality. If disclosed without permission, it could cause distress or damage and breach the person's privacy or human rights. Whatever you write may be disclosable.

Anything staff members post to external social media sites could reflect on the school and its work by virtue of your employment here. You should carefully consider what is posted in a personal capacity on, for example: Twitter, YouTube, Facebook, and LinkedIn.

Including a statement saying that the views expressed are your own does not absolve you of your responsibilities in relation to this. You must also refrain from making any reference to others in their capacity as employees or students (and parents) of the school and you should not befriend parents or students on social media.

The school could be considered "vicariously liable" (i.e. responsible) for anything that you write using school systems or by any method that identifies people connected to the School.

- Staff must not use, communicate, download, upload or access anything that could damage the schools', Trust, or their own, reputation or could be considered a breach of confidentiality, defamatory or harassment.

Staff should not contact parents/carers or students outside of the school's formal or agreed communication methods, for example staff should not text or WhatsApp message these.

Please remind yourself of the school's Code of Conduct and Data Protection Policy (on the school's website) and the confidentiality provision in your contract of employment.

To summarise:

- Don't write anything about students, parents/carers or staff of the school on social media (Facebook etc.)
- Don't use apps such as WhatsApp to communicate about students, parents or staff of the school
- Be careful what you send by email and text – everything you write has the potential to be shown to/seen by others. Texts should not include names or personal details about staff, students or parents/carers
- Writing inappropriate comments or giving personal information could get you and the school into trouble
- Take great care to check emails have been addressed correctly. Be wary of auto correct and auto completion features

- If in doubt, don't write it

All staff are required to check their school email accounts and read the weekly staff newsletter Enews on a regular basis for updates and important information.

Teams may set up WhatsApp groups for informal messaging but must ensure disappearing messages are enabled. Formal school business should not be communicated via WhatsApp. School email should be used to communicate formal school business.

Some team members may not wish to be part of a WhatsApp group; it is important that they don't miss out on any essential team information – alternatives are email and a text informing them that an email message has been sent. All team members should have access to the same information on school-related matters and line managers are to ensure that this happens through appropriate channels. Messaging out of hours can also disrupt work/life balance which all staff are encouraged to be mindful of.

Staff should remain mindful of their digital footprint and exercise caution in all their use of social media or any other web-based presence they have. This includes written content, videos or photographs and views expressed either directly or by 'liking' certain pages or posts or following certain individuals or groups. In addition, care must be taken when using dating websites where staff could encounter students of adult age or past students.