DIOCESE OF SOUTHWELL
& NOTTINGHAM
MULTI ACADEMY TRUST

MAGNUS
CHURCH OF ENGLAND
ACADEMY

SNMAT

Social Media Policy

Policy:	Social Media Policy
Approved by:	SNMAT Board of Directors
Date:	March 2026
Review Cycle:	Annual

Versions:			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2019		DO – IT Director	Initial version.
2020	May 2020	JS, DO, SKP	Policy reviewed and minor typos amended. Section on Fake News (page 6) has been removed.
2021	Oct 2021	DO	No changes required.
2022	May 2022	MY	Added references to supplementary document to support schools when setting up accounts. Page 5. Paragraphs numbered throughout the policy.
2022.6	June 2022	MY	Added specific instructions around professional communication, highlighting to stay away from WhatsApp.
2023	May 2023	MJH – IT Coordinator	Re-design, minor changes and fixed typos and structure. Updated definition of social media, examples and removed reference to Virtual Worlds. Amended scope, and consolidated “the aim of this policy is” with policy objectives. Added parent/carer responsibility to adhere to code of conduct. Added that staff need to understand how and where to report misuse to the social media platforms themselves. Added celebrating student/school achievements, parent comms, etc to best practises in education. Added recommendation to setup social media accounts with a shared mailbox rather than individual accounts. Moved professional communication from monitoring to responsible user of social media for staff.
2024	May 2024	MJH – IT Manager	Replaced school with academy throughout.

			Added note to ensure posted content adheres with safeguarding policies.
2025	April 2025	MJH	Minor formatting and spelling changes.
2026	03/2026	MJH	Added reference to align with Online Safety Act. Added scope to include social media checks and internet filtering for KCISE 2025. Add dis/misinformation safety risks. Added AI as a social media platform. Changed Twitter to X. Added Principal/Head responsibility to ensure compliance with eSafeguarding for filtering & monitoring. Expanding staff responsibilities for digital and online reputations.

INTRODUCTION

1. The widespread availability and use of social media brings opportunities to understand, engage and communicate in new and exciting ways. It is important that these technologies and services are used effectively whilst fulfilling the duty to safeguard children, young people and vulnerable adults. It is also important to ensure that their use meets legal, compliance and reputational responsibilities to SNMAT, the academies and the community.

2. This policy aligns with the Online Safety Act 2023-2025 which places legal duties on online platforms to protect children from illegal and harmful content.

SCOPE

This policy applies to:

1. Personal communications made via personal social media accounts where a personal account associates itself with, or impacts on, the Trust or academy;
2. Official social media communications posted at any time and from anywhere using any device;
3. Anyone who works with children/young people within the Trust, including consultants, contractors, casual and agency staff and volunteers (collectively referred to as staff in this policy).
4. Third parties who have access to SNMAT electronic communications systems and equipment.
5. Social media activity reviewed as part of safe recruitment checks in according with Keeping Children Safe in Education Guidance (KCSIE) 2025 (paragraph 225).

This policy does not apply to:

6. Personal communications which do not refer to or impact upon the Trust or academy.

OBJECTIVES

The aim of this policy is to:

7. Safeguard all children and young people in respect of the use of social media;
8. Protect the reputation of the Trust, its academies and staff and governors;
9. Protect the Trust, its academies and staff and governors from legal risks;
10. Ensure social media is used professionally, responsibly and safely;
11. Provide staff with guidance to what constitutes appropriate usage of social media;
12. Equip staff and students to recognise and respond to online misinformation and disinformation;
13. Remind staff that misuse of social media may be dealt with under disciplinary procedures and the most severe consequence of this could be dismissal.

DEFINITION OF SOCIAL MEDIA

14. Social media is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft, Roblox or World of Warcraft and video sharing platforms such as TikTok and YouTube have social media elements to them.

15. Social media examples include X, WhatsApp, Facebook, Instagram, TikTok, YouTube, Reddit, Xbox Live, LinkedIn and comment streams on public websites such as news sites.

16. Emerging technologies, including AI tools that enable content sharing or interaction (e.g. AI-powered chat platforms such as Grok or ChatGPT) may also constitute social media.

RATIONALE

17. Use of social media can pose risks to the Trust's ability to safeguard children and young people, protect its confidential information and reputation, and can jeopardise compliance with legal obligations.

18. The Online Safety Act imposes duties on online platforms related to harmful content, age assurance, and illegal activity. Staff must remain aware that these regulations do not eliminate risk and must stay vigilant when supporting children using online platforms.

19. All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation.

ROLES AND RESPONSIBILITIES

Board of Directors

20. The Board of Directors is accountable for the effective operation of the Social Media Policy overall. Regular reports around eSafeguarding in the academies are received by the Board which may reference social media where appropriate.

Local Governing Body

21. The responsibility for the effective operation of the policy in academies has been delegated to the Local Governing Body who will monitor and review its operation by receiving regular reports about social media Issues. It is recommended that the Safeguarding Governor includes the monitoring of social media within their remit.

Principal/Headteacher

22. The responsibility for the day-to-day operation of the Social Media Policy has been delegated to the Principal/Headteacher. The Principal/Headteacher is responsible for:

    - Ensuring that filtering and monitoring arrangements are in place as required by the SNMAT eSafeguarding Policy and KCSIE 2025;
    - Ensuring that all staff have read the policy and understand the standards expected of them;
    - Ensuring that effective training and advice is provided for staff;
    - Ensuring that all staff are aware of the procedures that need to be followed in the event of a social media misuse incident taking place;
    - Ensuring that a directory of all official social media accounts is maintained;
    - Reviewing and responding to any social media misuse incidents escalated to senior leaders.

Staff

23. All staff are responsible for ensuring that they:

    - Have read and understood this policy;

- Report any misuse of social media to the Principal/Headteacher;
- Direct any questions regarding the content or application of this policy to the Principal/Headteacher;
- Follow the guidance for good practise in the use of social media;
- Adhere to the expectations of professional conduct.

Parents/Carers

Parents/Carers are responsible for ensuring that:

- If they have access to an academy learning platform or social media account where posting or commenting is enabled, they should adhere to the SNMAT Code of Conduct for Parents, Carers and Visitors.

LINKING WITH OTHER POLICIES

24. The Social Media Policy must be read in conjunction with the other following policies:

- ICT Policy
- Bring Your Own Device (BYOD) Policy
- Data Protection Policy
- eSafeguarding Policy
- Artificial Intelligence Guidance
- Policy for Child Protection to Safeguard the Welfare of Children

GUIDANCE FOR IMPLEMENTATION

25. The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media professionally, responsibly, and safely to protect children/young people, staff and the Academy/Trust.

26. Social media can be used within the curriculum to support student learning, to celebrate Trust, academy and student achievements and to notify students and parents/carers of events.

27. Academies should be aware of which platforms are most popular and are being actively used by students and parents/carers.

28. Academies should know how and where to report misuse of social media on each platform and understand the relevant safety/privacy features.

29. Supplementary documentation detailing the recommended settings when creating and managing social media platforms should be followed – see Appendix 1.

Best Practises:

30. There should be a process for approval and review by senior leaders.

31. Distinct and dedicated social media sites or accounts held by a member of staff and separate from a personal account should be setup for educational purposes and linked to an official academy email account.

32. The URL, purpose and identity of academy social media sites should be notified to the Principal/Headteacher before launch and any access is permitted.

33. Clear processes for the administration and monitoring of accounts should involve at least two members of staff using an official academy email account, preferably a shared mailbox where responsibility can be easily transferred to another approved member of staff if required.

34. A code of behaviour, including procedures for reporting and dealing with misuse should be established.

35. The content of any official social media account should be solely for professional purposes and should reflect well on the Trust, its Academies and staff and students.

36. Any post on social media should be respectful and use an appropriate and professional tone.

37. Content should be reviewed to avoid sharing misinformation, disinformation or harmful narratives.

38. AI-generated content should be verified before posting, inline with SNMAT and DfE guidance.

39. Care should be taken so content does not breach copyright, data protection, safeguarding or any other legislation and that links to external sites are appropriate and safe.

40. No private messaging or other non-public method of communication or social media application or platform should be used.

41. Photographs of children or using any personally identifying information (including full names, named certificates, etc) should not be published without the explicit written consent of parents/carers in accordance with the Data Protection Policy.

42. If anyone, for any reason, asks not to be filmed or photographed or included in any social media post then their wishes should be respected.

43. Any misuse of social media should be reported to the Principal/Headteacher who should make a permanent record for evidence purposes (e.g., a screenshot) prior to removal.

44. All sanctioned social media accounts should include the Trust/Academy/Department official logo, approved images and have a link to the Trust/Academy website.

Responsible Use – Staff

45. It is acknowledged that in education staff may have children or other family members who attend their place or work or have friends that have children that attend their place of work. It is recognised in these circumstances there will be social communication between the member of staff and parents of other children and members of the Trust community. Where this applies, members of staff are advised:

    - Maintain a professional online reputation, understanding public profiles may be viewed by the SNMAT community;
    - To be particularly careful about keeping their social and work communications separate;
    - To ensure that all communications are with parents and not with children;
    - To inform the Principal/Headteacher so they are aware of the situation.

46. Do not use academy logos, branding, or imagery on personal accounts.

47. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not

communicating on behalf of the academy with an appropriate disclaimer.

48. Regularly check and evaluate their digital footprint, keeping personal information private and ensuring that accounts have the appropriate privacy settings applied.

49. Only use SNMAT provided systems O365, E-Mail and Teams for professional communication with colleagues and refrain from using personal social media platforms such as WhatsApp, Snapchat, Messenger/Facebook, iMessenger etc.

Responsible Use – Parents/Carers

50. If Parents/Carers have access to an academy learning platform or social media account where posting or commenting is enabled, parents/carers should adhere to SNMAT's Code of Conduct for Parents, Carers and Visitors.

51. Parents/Carers are encouraged to comment or post appropriately about the academy. In the event of any offensive or inappropriate comments being made, the academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the academy's complaints procedures.

MONITORING SOCIAL MEDIA USAGE

52. Online posts and mentions can have a severe impact on the reputation of the Trust, its academies, its staff and governors. As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the trust/academy. The academy should ensure a procedure is in place to effectively respond to social media comments made by others.

53. The Academy's use of social media for professional purposes should be checked regularly by the nominated responsible person to ensure compliance with Trust/academy policies.

54. Staff are reminded that social media postings and activities may be proportionately monitored as explained in the eSafeguarding and IT Policy.

APPROPRIATE USE GUIDE

APPROPRIATE	**INAPPROPRIATE**
Blocking unwanted communication from pupils.	Inviting, accepting friends requests or engaging in communications with pupils over social network sites.
Reporting communication received from children/young people on any personal social media sites to the Designated Safeguarding lead.	Accepting any current pupil of any age or any ex-pupil of the academy under the age of 18 as a friend, follower, subscriber or similar on any personal social media account or interacting on social network sites and forums.
Reporting any inappropriate communications involving any child in any social media to the Designated Safeguarding Lead.	
Verifying information, especially AI generated content.	Sharing misinformation, disinformation or harmful narratives.
Setting all privacy settings to the highest possible levels on all personal social media accounts.	Posting disparaging or defamatory statements about: • the Academy/Trust;

	• the students or their parents or carers; • the Directors, governors or staff; • suppliers and vendors; and • other affiliates and stakeholders.
Using an official academy e-mail account for all email communication on academy business with staff and members of the academy community.	Posting comments about specific individual matters and sensitive Academy/Trust-related topics.
Ensuring that your profile and any content you post are consistent with the professional image you present to pupils/students and colleagues.	Using academy/Trust logos, brand names, slogans or other trademarks, or post any of their confidential or proprietary information without prior written permission.
Making it clear that your views do not represent those of the Trust/academy.	Circulating chain letters, other spam, commercial, personal, religious, or political solicitations, or promotion of outside organisations unrelated to the Academy/Trust's business at work.
Refraining from making a communication if you are in any way uncertain about the appropriateness of the content and checking with the Principal/Headteacher.	Using social media in any way that would breach any other Trust or academy policies.
Printing out any content in social media that disparages or reflects poorly on the Academy/Trust or its stakeholders and contacting the Headteacher/Principal about it.	Providing references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Academy/Trust and create legal liability for both the author of the reference and the Academy/Trust.
Referencing sources of particular information you post or upload where appropriate and citing them accurately to protect yourself and the Academy/Trust against liability for copyright infringement. Asking the Principal/Headteacher if you have any questions about whether a particular post or upload might violate anyone's copyright or trademark before making the communication.	

REVIEW

55. This policy is reviewed annually by SNMAT in consultation with recognised trade unions. The application and outcomes of this policy will be monitored to ensure that it is working effectively.

APPENDIX 1 – SOCIAL MEDIA CHECKLISTS

Downloadable guidance on how to configure profile settings in various social media platforms:

https://swgfl.org.uk/resources/checklists/

APPENDIX 2 – SOCIAL MEDIA BEST PRACTISES FOR PARENTS/CARERS

Best practices for parents and carers to stay safe online when using social media.

https://saferinternet.org.uk/online-issue/social-media-3