



Social Media Policy

Adopted By: Board of Trustees

Date: September 2025

Review Date: September 2026

Social Media Policy

Date of Issue:	September 2025
Policy applies to:	All staff employed by the Wessex Multi-Academy Trust.
Policy Version Number:	03
Purpose of the document:	To provide guidance and expectations surrounding the safe and acceptable use of social media.
Summary of the main points:	The document provides: 1. An overview into safer social media practice across the Trust. 2. An overview into roles and responsibilities across different categories of people.
Approved by:	The Board of Trustees
Reviewer:	Sophia Radford - DPO
Summary of amendments:	1. Amendment to para 1.2 2. Additions to paras 8.1.6, 8.2.3, 8.2.9, 8.3.1 and 8.3.4 3. New para 8.2.11 4. New section 14 re cyber security and privacy
Next review due:	September 2026

Contents

Section	Page
1. Introduction	4
2. Scope	5
3. Status	5
4. Principles	5
5. Roles and Responsibilities	6
6. Definitions	7
7. Data Protection Principles	7
8. Staff Social Media Use	8
8.1 School Accounts	8
8.2 Personal Accounts	11
8.3 Parents Social Media Use	12
8.4 Pupil Social Media Use	12
9. Online Safety	13
10. Blocked Content	14
11. Cyber Bullying	14
12. Training	14
13. Monitoring	15
14. Breach of the Policy	15
15. Review	15

Appendices

1. Relevant legislation	16
-------------------------	----

1. Introduction

- 1.1 This document sets out Wessex Multi-Academy Trust's (WMAT) policy on social media. WMAT understands that social media is a growing part of life both within and outside our schools. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for Trust staff in many ways. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

This policy aims to:

- Promote the responsible use of social media by all staff, parents and pupils in support of the Trust's and its school's values and vision.
 - Assist Trust staff working with children and young people to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
 - Set clear expectations of behaviour and/or codes of practice relevant to social media for educational, personal or recreational use.
 - Support safer working practice.
 - Encourage positive interactions with social media for both pupils and staff and promote respectful behaviour for all users of social media
 - Safeguard the reputation of the Trust through irresponsible use of social media.
- 1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. It is expected that where matters arise that are not covered in this policy staff will always advise the Headteacher and seek guidance for the appropriate action to be taken. Headteachers will in turn seek advice from HR where appropriate.
- 1.3 This policy takes account of employment legislation and best practice guidelines in relation to social media in addition to the legal obligations of School Governance Committees and the relevant legislation listed in Appendix 1.
- 1.4 All Trust employees must adhere to and apply the principles of this policy in all aspects of their work. Failure to do so may lead to action being taken under the Disciplinary Procedure, up to and including dismissal.
- 1.5 For the WMAT Central team, references to schools should be replaced with Head Office.
- 1.6 Throughout this document, references to Headteacher also include Head of School.

2. Scope

- 2.1 This policy applies to all staff within the Trust. This includes teaching staff, support staff, supply staff, local governors, trustees, central team staff, contractors and volunteers.

- 2.2 This policy should be followed by any adult whose work brings them into contact with children or young people. References to staff should be taken to apply to all the above groups of people within the Trust. Reference to children and young people means all pupils at school including those over the age of 18.
- 2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example, any alleged misconduct which falls within the scope of the Dealing with Allegations of Abuse against Staff and Volunteers Policy requires the Trust to comply with additional child protection requirements set out in that policy.
- 2.4 Where appropriate, staff should refer to other relevant policies in relation to data protection, equality, bullying and harassment.
- 2.5 This policy is non-contractual and the Trust may amend, update or supplement it at any time. The Trust will notify staff of any new or modified policy when it is adopted.

3. Status

This document does not replace or take priority over advice provided by HR, the Designated Safeguarding Lead (or where appropriate the deputy) or the Trust's Staff Code of Conduct, Dealing with Allegations of Abuse, or other policies issued around safeguarding or IT issues (e-mail, ICT and data protection policies) but is intended to both supplement and complement any such documents.

4. Principles

- Adults who work with children and young people are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Staff across the Trust should work and be seen to work in an open and transparent way.
- Staff across the Trust should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance within this policy.

5. Roles and Responsibilities

Headteacher/Senior Leadership Team are responsible for:

- Ensuring all staff, parents and pupils are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Ensuring this policy, as written, does not discriminate on any grounds, including against any of the protected characteristics, as outlined in the Equality Act 2010.

- In conjunction with the School Governance Committees and/or Board of Trustees, handling complaints regarding this policy and its provisions in line with the Trust's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.

The Board of Trustees are responsible for:

- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an agreed basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

Staff members are responsible for:

- Adhering to the principles outlined in this policy.
- Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff or pupils to the Headteacher/CEO immediately.
- Attending any training on social media use offered by the Trust.

IT are responsible for:

- Providing technical support in the development and implementation of media accounts.
- Implementing appropriate security measures as directed by the CEO/Board of Trustees.
- Ensuring the Trust's filtering and monitoring systems are updated as appropriate.

6. Definitions

For the purpose of this policy, social media refers to any online platform that offers real-time interaction by creating and exchanging content between the user and other individuals or groups including, but not limited to, the following:

- Blogs
- Online discussion forums such as NetMums
- Collaborative spaces such as Facebook, LinkedIn
- Media-sharing devices such as YouTube, Snapchat, Instagram or Tik Tok
- 'Micro-blogging' applications such as X

For the purpose of this policy, "**cyberbullying**" is defined as any social media or communication technology intentionally used to bully an individual or groups, including the posting or sharing of messages, images or videos.

For the purpose of this policy, **"members of the Trust community"** are defined as any teacher, members of support staff, pupil, parent of a pupil, local governor, Trustee or ex-pupils.

7. Data Protection Principles

- 7.1 The Trust will obtain consent from pupils and parents via the data collection exercise for joiners carried out by individual schools. The consent will remain valid for the duration of time that the pupil remains at the individual school however this can be removed at any time by notifying the individual school. Consent provided for the use of images and videos only applies to Trust/school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.
- 7.2 Where a pupil is assessed by their individual school to have the competence to understand what they are consenting to, the school will obtain consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the pupil.
- 7.3 A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The Data Lead in each individual school is responsible for ensuring this consent record remains up to date.
- 7.4 Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the individual school in writing. Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and pupils' requirements following this. Wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.
- 7.5 Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided. The individual school will only post images and videos of pupils for whom consent has been received.
- 7.6 Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the School's IT Department for use. Only appropriate images and videos of pupils will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- 7.7 When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.
- 7.8 When posting images and videos of pupils, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified where consent has not been provided. The school will not post pupils' personal details on social media platforms and pupils' full names will never be used alongside any videos or images in which they are present.

7.9 Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

7.10 Any breaches of the data protection principles will be handled in accordance with the Trust's Data and Cyber-Security Breach Prevention and Management Plan.

7.11 Where consent has been provided, images may be utilised by WMAT for the purposes of advertising or marketing, for example the use of banners or on the Trust web site.

8. Staff Social Media Use

8.1 School accounts

8.1.1 Individual school's social media sites will only be created and monitored by staff members designated and approved by the Headteacher. There will be a strong pedagogical or business reason for the creation of social media accounts on behalf of the individual school; official school profiles and accounts will not be created for trivial reasons.

8.1.2 If members of staff wish to create a new social media account, they will seek approval from the Headteacher.

8.1.3 A school social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account. This policy does not seek to regulate how staff use social media in a purely private capacity, provided that use has no bearing on the Trust, individual schools or their activities. This policy is intended to ensure that staff understand the rules governing their use of social media in relation to their work for the Trust/ and or school, or when referencing the Trust/and or school, or where use of social media may affect the Trust/ and or the individual school or its activities. It is designed to help you use these platforms and services responsibly, so as to minimise the risks set out above and to ensure consistent standards of use of social media. This policy therefore applies where:

- Staff use of social media relates to the Trust/ and or the individual school or its activities;
- Staff use of social media relates to, or is otherwise connected with, their work, whether the intended use is personal or professional; and/or
- staff represent themselves, or are otherwise identifiable, as someone employed by, or otherwise associated with, the Trust and or the individual school.

8.1.4 Consideration will be given to the following aspects:

- The purpose for using social media
- Whether the overall investment will achieve the pedagogical aim
- The level of interactive engagement with the site

- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the proposed site
- A clear plan which outlines aspects such as how long the site will last
- How the success of the site will be evaluated

8.1.5 School social media passwords are stored by the Headteacher (in some schools this may be delegated to an appropriate person) – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the Headteacher. Staff will adhere to the data protection principles outlined in **Section 7** of this policy at all times.

8.1.6 Any social media accounts should have a nominated point of contact who is responsible for content posted on to the account. Only authorised members of staff shall be authorised to post to school media accounts. Staff will ensure any posts are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience; positive in nature and relevant to pupils, the work of staff, the school or any achievements. Staff will not post any content online which is damaging to the school, any of its staff or pupils or the Trust.

8.1.7 All content expressed on school social media accounts will not breach copyright, data protection or freedom of information legislation.

8.1.8 Staff will ensure the Headteacher (or appropriate designated person) has checked the content before anything is posted on social media. If staff wish for reminders to be posted for parents, e.g. returning slips for a school trip, staff will seek permission from the Headteacher (or appropriate designated person) before anything is posted.

Staff must not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by the Trust.

8.1.9 If inappropriate content is accessed online, it will be reported to Oakford Technology (where services are purchased) or the School IT Technician immediately. The Trust retains the right to monitor staff members' internet usage in line with the Data and Cyber-security Breach and Management Plan.

If staff become aware of adverse criticism of the Trust/ and or a school, or of content staff have created or shared they must inform their line manager. Staff should not respond without the express approval of their line manager.

8.1.10 The school's social media accounts will comply with the relevant site rules at all times, particularly with regards to the minimum age limit for use of the site. It will be noted that each networking site has their own rules which must be followed – the appropriate member of staff will induct staff to each new social media platform, providing them with the relevant training and information.

8.2 Personal Accounts

- 8.2.1 Staff members will not access social media platforms during lesson times, but they are permitted to use social media during break times in designated areas. Staff will avoid using social media in front of pupils at all times.
- 8.2.2 Staff members will not use any school or Trust owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the Headteacher. Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the Headteacher, and once Oakford Technology (where services are purchased) or the School IT Technician has ensured the necessary network security controls are applied. Staff must not use their work email address to sign up for personal use of social media platforms.
- 8.2.3 Staff will not message, 'friend', 'follow' , react to social media posts, or otherwise contact pupils or parents through their personal social media accounts. If pupils or parents attempt to message, 'friend' or 'follow' a staff member, they will report this to the Headteacher. Due to living in a small community, there may be occasions when there are social contacts with pupils or parents through personal social media accounts, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged and where this may not be easily recognised the staff member must notify the school. There must be awareness on the part of those working with pupils that some social media contacts, especially where these are not common knowledge, could be misconstrued. This can also apply to social media contacts made through outside interests or through the staff member's own family.
- 8.2.4 Staff members will not provide their home address, phone number, mobile number, social networking details or e-mail addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels. Staff members will use their school or Trust e-mail address for school/Trust business and personal e-mail address for their private correspondence; the two should not be mixed.
- 8.2.5 Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school or Trust on their personal social media accounts. Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not those of the school/Trust.
- 8.2.6 No staff member will post any content online that is damaging to the school/Trust or any of its staff or pupils. Staff members will not post any information which could identify a pupil, class or an individual school – this includes any images, videos and personal information. Staff will not take any posts, images or videos from social media that belong to the school/Trust for their own personal use. Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- 8.2.7 Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. Members of staff will be aware that if their out-of-work activity brings the Trust into disrepute, disciplinary action will be taken.

- 8.2.8 Attempts to bully, coerce or manipulate members of the Trust community via social media by members of staff will be dealt with as a disciplinary matter in accordance with the Trust's **Disciplinary Policy and Procedure**.
- 8.2.9 Social media will not be used as a platform to attack, insult, abuse or defame pupils, their family members, colleagues or other professionals. All users of social media must use respectful language and refrain from using derogatory, discriminatory, or offensive language when posting or commenting on social media.
- 8.2.10 Staff members' personal information will not be discussed on social media. 8.2.11 Staff should be aware that they have no expectation of privacy or confidentiality in anything they create or share on social media platforms. When staff create or exchange content using social media they are making a public statement. As such, staff should be aware that their content will not be private and can be retweeted, copied or forwarded to third parties without their consent.
- 8.2.11 Staff who have any professional social media presence should be aware that they are representing the school when they post, comment or like something.

8.3 Parent Social Media Use

- 8.3.1 Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school or Trust. Parents should engage in positive online interactions and respectful behaviour at all times when engaging with school social media.
- 8.3.2 Parents will be asked not to share any photos or personal details of pupils when commenting on any school social media sites, nor post comments concerning other pupils or staff members, in accordance with the Parent & Community Code of Conduct.
- 8.3.4 Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the Headteacher and may have their ability to interact with the social media websites removed. Parents should immediately report any breaches of this policy to the Head Teacher / Wessex MAT.
- 8.3.5 Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

8.4 Pupil Social Media Use

- 8.4.1 Pupils are not permitted access to social media during the school day unless it is part of a curriculum activity and permission has been granted. Pupils are not permitted to use their school's WiFi network to access any social media platforms unless prior permission has been sought from the Headteacher, and the School IT Technician has ensured appropriate network security measures are applied. Schools with 6th Form students may allow those students to carry mobile phones during the day however usage will be limited to break times or free periods and only when in designated areas.

- 8.4.2 Pupils will not attempt to message, 'friend', 'follow' react to any staff posts, or otherwise contact members of staff through their personal social media accounts. Pupils are only permitted to be affiliates of school social media accounts. Where a pupil or parent attempts to message, "friend" or 'follow' a staff member on their personal account, it will be reported to the Headteacher.
- 8.4.3 Pupils will not post any content online which is damaging to the school/Trust or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.
- 8.4.4 Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.
- 8.4.5 If inappropriate content is accessed online on school premises, it will be reported to a teacher.
- 8.4.6 Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to exclusion.

9. Online Safety

- 9.1 Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.
- 9.2 Concerns regarding a staff member's online behaviour will be reported to the Headteacher, who will decide on the best course of action in line with the relevant Trust policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it will be reported to the Chair of Governors.
- 9.3 Concerns regarding a pupil's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the Headteacher and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.
- 9.4 Where there is a concern that illegal activity has taken place, the Headteacher will contact the police. The Trust will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.
- 9.5 As part of the usual communication with parents, the Trust will reinforce the importance of pupils being safe online and inform parents what systems are used to filter and monitor online use. Individual schools will also make it clear to parents what their children are

being asked to do online for school including what sites they will be asked to access and who from the school, if anyone, they will be interacting with online.

10. Blocked Content

- 10.1 In accordance with the Trust's Data and Cyber-security Breach Prevention and Management Plan, the Trust's IT Department will install filtering systems on the school's network to prevent access to certain websites. Social media websites are not accessible on the school's network including but not limited to Facebook, Snapchat, X and Instagram.
- 10.2 The Trust's IT Department retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.
- 10.3 Attempts made to circumvent the network's firewalls will result in a ban from using Trust computing equipment, other than with close supervision.
- 10.4 Inappropriate content accessed on the Trust's computers will be reported to Oakford Technology (where services are purchased) or the School IT Technician so that the site can be blocked. Requests may be made to access blocked content by submitting a blocked site for review via a form on the block page of the Trust's web filter page.

11. Cyberbullying

- 11.1 Cyberbullying incidents are taken seriously at the Wessex Multi-Academy Trust. Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.
- 11.2 Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members who feel that they have been harassed or bullied because of material posted or uploaded by a colleague onto a social media platform will be handled in accordance with the Allegations of Abuse Against Staff Policy.

12. Training

- 12.1 The Trust recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils. Staff will receive training on social media as part of their new starter induction. Teachers and support staff will receive ongoing training as part of their development.
- 12.2 Pupils will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links. Pupils will be provided with material to reinforce their knowledge.

- 12.3 Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

13. Monitoring

- 13.1 The Trusts internet and E-Safety Policy, in particular in relation to the Trusts right to monitor, intercept and read communications, applies equally to use of social media platforms via the Trust's systems or network.
- 13.2 The Trust will also monitor how the Trust and its individual schools use social media generally and what is said about us. Oakford Technology is responsible for this monitoring.

14. Cybersecurity and Privacy

- 14.1 Staff must protect the school social media accounts and ensure they comply with passwords and security settings. Staff make themselves aware of privacy settings and use them appropriately to protect content.
- 14.2 Staff must not share sensitive personal information, such as addresses or phone numbers, on public social media platforms.
- 14.3 If any member of staff suspects a breach or unauthorised use of any social media accounts, they must report it immediately to the Headteacher and/ or Wessex MAT.

14. Breach of the Policy

- 14.1 The Trust considers this policy to be extremely important. If any staff are found to be in breach of the policy, they will be disciplined in accordance with the Trust's Disciplinary Policy and Procedure. In certain circumstances, breach of this policy may be considered gross misconduct, which may lead to immediate termination of employment without notice or payment in lieu of notice. As an alternative, the Trust may withdraw staff access to social media platforms via its systems. If any parent/ pupil is in breach of this policy this may result in suspension of access to the Trust social media platforms.

15. Review

In this first instance, this policy will be reviewed on an annual basis as a new policy document. It will then be subject to a review every three years.

Any changes to this policy will be communicated across the Trust.

Links to other policies

Disciplinary Policy and Procedure
Child Protection and Safeguarding Policy
Fairness and Dignity at Work Policy Staff Code of Conduct
Data Protection

Appendix 1 – Relevant Legislation

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- DfE (2018) – ‘Data protection: a toolkit for schools’
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- DfE (2022) ‘Keeping children safe in education 2024’