Social Media Policy

Approved by: Trust Board	Date: 19.07.24
Last reviewed on: 10.10.25	
Next review due by: 10.10.26	

Updates and amendments

Date	Policy section	What's changed?	Why?

Contents

Version control

Version	Date	Author	Changes
June 2023	September 2023	M Ridsdale	Policy reviewed and typo changes amended – section on Code of Conduct Social networking type word around unconsented images
October 2023	October 2023	M Ridsdale	Policy reviewed in response to 'auditor findings and recommendations' Added new references to Roles and responsibilities and specific reporting accountability process map should a breach occur. Passwords update changed to every 60 days from the previous 90 days.
July 2024	July 2024	M Ridsdale	Date change on policy Addition of Trust Safeguarding Lead in Roles and Responsibilities

Objectives

This policy sets out Forward As One CE MAT's policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in any social networking sites such as Facebook or Twitter and posting material, images, or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image.

In addition, Forward As One CE MAT has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key principles

All members of Forward As One CE MAT have a responsibility to ensure that they protect the reputation of the Trust and the schools that sit within, and to treat colleagues and members of the school with professionalism and respect.

It is important to protect everyone at Forward As One from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is paramount and is a key responsibility of all members of staff and it is essential that everyone at Forward As One considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the MAT either as a paid employee or volunteer must not communicate with children via social networking.

With safeguarding in mind, staff, parents and visitors are prohibited from using mobile phones in public areas around school and on school premises.

This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Headteacher/CEO.

It is also completely unacceptable to communicate on social media about the MAT or any member of the school community in or out of work on personally owned equipment.

Aims

- To set out the key principles and code of conduct expected of all members of staff, governors and volunteers at Forward As One CE MAT with respect to social networking.
- To further safeguard and protect children and staff.

Overview and Expectations

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct to maintain the confidence and respect of their colleagues, children, public in general and all those with whom they work.

Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting. The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with children.

Anyone whose practice deviates from this document and/or their professional or employmentrelated code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication

technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

Code of Conduct: Social Networking

Under no circumstances should staff refer to any staff member, pupil, parent or Trust / school activity/event.

The following are also **not considered acceptable** at Forward As One CE MAT

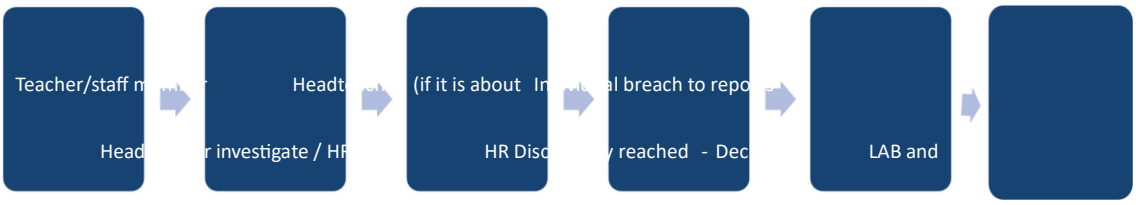
- The use of the Trust or school's name, logo, or any other published material without written prior permission from the CEO / Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the Trust / school to any form of illegal conduct, or which may damage the reputation of the Trust / school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of any **unconsented images** of employees, children, governors, trustees or anyone directly connected with the Trust / school whilst engaged in school activities.
- Trust / school social media accounts and their administration is by **designated authorised personnel only** and is under the direction of the CEO/COO /Headteacher.

In addition to the above everyone at Forward As One CE MAT must ensure that they:

- Communicate with children and parents in an open and transparent way using the Trust / school phone number and email address.
- Never 'friend' a pupil at the Trust / school where they are working onto their social networking site.
- Do not make any derogatory, defamatory, rude, threatening, or inappropriate comments about the Trust / school, or anyone at or connected with the Trust /school.
- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the Trust / school's reputation is compromised by inappropriate postings.
- Any views or opinions expressed by employees on any form social media is their own personal view and not representative of the Trust / school.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.
- Make sure that high levels of privacy are set if they choose to use social media.
- Passwords for social media accounts should be **updated every 60 days.**
- Mobile phones must not be used on the premises by parents and carers.

Roles and Responsibilities

Potential and Actual Breaches of the Code of Conduct



In instances where there has been a breach of the Code of Conduct, the above will apply:
Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure.
A breach of this policy will be a serious disciplinary offence which is also contrary to the Trust / school's ethos and principles.
The Trustees will take appropriate action to protect the Trust / school's reputation and that of its staff, parents, governors, children, trustees and anyone else directly linked to the school.
Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the CEO / Headteacher of the justification for any such action already taken or proposed. The CEO / Headteacher will in turn seek advice from Human Resources where appropriate. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation.

Safer Online Behaviour

Some social networking sites and other web-based sites have fields in the user profile for job title etc. **If you are an employee of the Trust and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the Trust /school where you work. In some circumstances this could damage the reputation of the Trust / school, the profession or the local authority.**

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for children or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties. All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the school, or another school, Manchester Diocese or Bolton/Bury/Tameside / Oldham / Lancashire Council could result in formal action being taken against them. This includes the uploading of photographs which might put the Trust / school into disrepute.

Mobile Phones/Camera/Video Recorder Usage

To ensure the safety and welfare of children in our care personal mobile phones, cameras, ipads and video recorders must not be used when children are present.

- All mobile phones must be kept in a secure place, switched off and not be accessed throughout contact time with the children.
- In exceptional circumstances, which have been discussed and agreed with a member of the leadership team, staff may keep their phone switched on and accessible as long as they use their phone out of view of children, i.e. in a room designated for staff, e.g. the staff room, an office or the PPA room.
- During school visits mobile phones should be used away from the children and for emergency purposes only.
- Photographs or images of any children within our care may only be taken following parental consent and only using one of the school cameras / i-pads. These images should remain within this setting or be shared only with the parents of the child concerned.
- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.
- School photographs and recordings can only be transferred to and stored on a school computer.

Protection of Personal Information

Staff should not give their personal e-mail addresses to children or parents.
Where there is a need for communication to be sent electronically the school e-mail address should be used. Likewise, staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity. There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are

part of the same social circle or members of the same parish or community. These contacts, however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the senior leadership team.

Staff should never share their work logins or passwords with other people.

Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making, and storing indecent images of children are illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which can lead to a criminal prosecution. Where other unsuitable material is found, which may not be illegal, but which raises concerns about that member of staff, the Headteacher (and in the Head's absence, a member of the SLT) should be informed and that person will seek advice from HR. The school will not attempt to investigate or evaluate the material themselves until such advice is received.

Cyber-bullying

Forward As One CE Mat's definition of cyber-bullying is 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyber-bullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site. Staff are encouraged to report all incidents of cyber-bullying to their line manager or the Headteacher/CEO. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Guidance for Implementation

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

Best Practice in the use of social media for educational purposes

Social media can be used within the curriculum and to support pupils' learning. for example, the school may have an official blog or Twitter account.

The following practices should be observed:

- There should be a process of approval by the Headteacher.
- Distinct and dedicated social media sites or accounts, entirely separate from any personal social media accounts held by member of staff, should always be set up for educational purposes which should be linked to an official school email account.
- Clear processes for administration and monitoring of these accounts should be in place.
- The content should be solely professional and should reflect well on the school/Trust.
- Any inappropriate comments on, or abuse should be immediately reported to the Headteacher who should make a permanent record for evidence purposes 9e.g., screen shot) prior to removal.

Link with Other Policies

This policy should be read in conjunction with the following:

- Safeguarding and Child Protection Policy
- Data protection Policy
- Online Safety Policy
- Equality Duty
- Whistleblowing Policy
- Acceptable Use of IT Policy

Review of Policy

Due to the ever-changing nature of information and communication technologies it is best practice that this policy be reviewed annually.