Social Media Policy

Policy Owner:	SHINE Academies CEO
Policy Date:	December 2023

This policy has been agreed as being fully consulted on with the following trade unions ASCL, NAHT, NASUWT, Unison, NEU, GMB and UNITE and was implemented by SHINE Academies on the above date

CONTENTS

1. Introduction

1 This policy sets out Shine Academies approach to employee use of social media. It is acknowledged that all employees have a right to use social media in their personal lives, however everything shared on a social networking site could potentially end up in the worldwide public domain and be seen or used by someone the employee did not intend, even if it appears to be 'private' or is on a closed profile or group.

1.2 It is recognised that Social Media landscapes have the potential to be misused. Employees who fail to respect the rights and entitlements of individuals will be subject to appropriate processes and procedures.

2. Background

2.1 This policy will:

- Protect the Trust against liability for the actions of its employees
- Help ensure that all employees are aware of their responsibilities in regard to social media use
- Legal framework: this policy has due regard to legislation and guidance including, but not limited to Human Rights Act 1998(amendment) order 2004, Public Interest Disclosure Act 1998, Equality Act 2010, Data Protection Act 2018 (GDPR), CCTV and Code of Practice 2010, Computer Misuse Act 1990 (amended 2015), Copyright, Design and Patents Act 1988 and Investigatory Powers (Consequential amendments etc.) Regulations 2018
- Promote safer working practices and standards with regards to the use of social media
- Establish clear expectations of behaviour in social media use
- Make clear to users who they should contact about any particular aspect of the policy
- Notify users of any privacy expectations in their communications

3. Purpose of Policy

3.1 The aim of this policy is to help protect the Trust against liability for the actions of its employees, and help employees draw a line between their private and professional lives by setting out rights, responsibilities and limitations which will help the Trust prevent any unauthorised comments which might result in creating a legal risk.

3.2 This policy is intended to help employees make appropriate decisions about the use

of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, or comments on web-articles, such as Twitter, Facebook, YouTube, Instagram, TikTok, and LinkedIn, and messaging platforms such as WhatsApp (this list is not exhaustive and the Trust recognise that this is a constantly changing canvas).

3.3 This policy outlines the standards the Trust require employees to observe when using social media, the circumstances in which the Trust will monitor employee use of social media and the action the Trust will take in respect of breaches of this policy.

3.4 This policy establishes core standards of behaviour for the use of social media for both personal and professional use. The Trust expects employees to follow the accepted norms of behaviour when using any social media sites; for example, if comments or pictures circulated within the staffroom would not be acceptable, or any other behaviour in a face-to-face workplace would be deemed inappropriate, it will be unacceptable online.

4. Who is Covered by the Policy

4.1 This policy covers all individuals working at all levels and grades within the Trust including: Chief Executive Officer, Director of Operations, Headteachers, senior leadership team members, teachers, support staff, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as employees in this policy).

4.2 Unless otherwise stated, this policy and procedure applies to all employees of SHINE Academies. Where the term employee is used throughout the policy this applies to both employees and workers. The exception to this is that where an employee has transferred into the Trust under TUPE and has enhanced pay terms. The enhanced TUPE terms will apply (subject to any other changes that may occur from time to time by agreement and/or under operation of TUPE).

5. The Scope of the Policy

5.1 All employees are expected to comply with this policy at all times to protect the privacy, confidentiality, and interests of the Trust, employees, parents, pupils, and any other individual with an association to the Trust.

6. Application

6.1 The policy applies to use of the internet and mobile technologies (such as smart phones/texting/internet and emails/social network sites/blogging and tweeting) whilst outside of the workplace both public and in-house.

6.2 Only the Chief Executive Officer or designated persons are permitted to post material on a social media website in the Trust's name. Any breach of this policy may be subject to disciplinary processes.

7. Responsibilities

7.1 The Chief Executive Officer has overall responsibility for the effective operation of this policy.

7.2 The Chief Executive Officer, along with the Trust Board, is responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to the Trust.

7.3 All employees are responsible for their own compliance with this policy and for ensuring that it is consistently applied. All employees should ensure that they take the time to read and understand it. Any breach of this policy should be reported to the Chief Executive Officer, Headteacher or Director of Operations in the first instance. Concerns relating to the Chief Executive Officer should be reported to the Chair of the Trust Board.

7.4 Teaching staff must have regard for the Teaching Standards and all employees must recognise the principles of the Trusts Staff Code of Conduct.

7.5 Questions regarding the content or application of this policy should be directed to the Trust's HR provider.

7.6 Everything written on social networking sites is in the public domain, even where privacy settings are set, or material is posted on a closed profile or group.

7.7 Employees must use internal mechanisms to voice concerns (i.e., Grievance, Whistleblowing Procedures) about issues relating to work generally, or their place of work or anything else related to work. Raising these issues outside the workplace may damage the reputation of the organisation.

7.8 Employees must:

- Not disclose personal details or identify their geographical location (by disabling access to their geo location to other users), including the publication of photographs where consent has not been given or where it can be reasonably assumed that consent would not be given
- Choose online 'friends' carefully – this must NOT include pupils or recent pupils. Remember privacy cannot be guaranteed. If an employee is 'friends' with parents, the employee must not discuss anything relating to the business of the Trust and ensure that confidentiality is maintained at all times
- Ensure that privacy settings remain unchanged. Privacy settings are not infallible and employees should be aware that items shared on social media may become more widely available than intended by the person posting

- Not make references to places of work, the Trust, publicise work or private - telephone numbers, addresses or e-mail addresses
- Not share confidential information or private data relating to knowledge obtained through their employment with the Trust
- Ensure that online activities do not interfere with their job, colleagues or commitments to pupils and their parents/carers
- Ensure that if identifying themselves as a Trust employee, social media profiles and related content is consistent with how they wish to present themselves with colleagues, pupils and their parents/carers
- Ensure responsibility in reading content carefully before liking a post or posting other emojis to identify an opinion
- Not subject colleagues to any use of inappropriate or unwanted political or personal reference either in writing, videos, photographs, text messaging, voice notes, posting blogs, or email that reveal some form of work-related behaviour (known as Cyber bullying - to support deliberate and hostile attempts to hurt, upset or embarrass another person). Further guidance on Cyber bullying can be found in Appendix 1
- Not compromise the Trust or colleagues by making adverse, damaging or libellous comments, using social media to express views (negative or positive) with which the Trust would not wish to be connected, which are prejudicial to the best interests of the Trust and its employees or contravene the Teacher's Standards
- Care should be taken if using social networking sites to screen candidates during recruitment activities. Any online employment checks should be completed in line with Keeping Children Safe in Education and Safer Recruitment.
- Anyone who identifies themselves as a Trust employee will be required to use a disclaimer on any blogs, for example, stating that "all views are my own and do not necessarily reflect the official position of my employer"
- Not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content
- Never discuss the Trust, pupils or parents/carers on social media
- Be aware of discussing topics that may be inflammatory

7.9 If an employee is a victim of online abuse, they should not respond in any way to the material but must report it to their manager at the earliest opportunity.

8. Policy Breaches

8.1 Employees found to be in breach of this policy may be subject to disciplinary action, in accordance with the Trusts Disciplinary Procedure, which can be located on the Shared Policy Area, with possible sanctions up to and including dismissal.

8.2 Information shared through social media sites, even on private platforms, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

9. Monitoring

9.1 Employers may have legitimate concerns about security that in some way justify a degree of monitoring whilst acknowledging the protection of employee's rights and privacy. Monitoring should only take place where it is needed to prevent specific illegal or defamatory acts and consideration should be given to any counterproductive effects of the monitoring. Employees must be fully aware of what the Trust monitor, how they go about it and why they do so.

9.2 If it becomes apparent through monitoring or other means (whether or not accessed for work purposes), that an individual has acted in a manner that conflicts with this policy, then the Trust should invoke the Disciplinary Procedure, which can be located on the Shared Policy Area. According to the seriousness of the offence, this could result in action that may ultimately lead to dismissal or further referral processes to other agencies such as safeguarding. For certain offences, the individual may also be liable for prosecution under the Computer Misuse Act 1990 (amended 2015), the Data Protection Act 2018 (GDPR).

9.3 Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against an employee and the organisation. It may also cause embarrassment to the Trust, its pupils and its parents/carers.

9.4 In particular uploading, posting, forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, may amount to gross misconduct and could potentially result in dismissal under the Trusts Disciplinary Procedure (this list is not exhaustive):

(a) Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)

(b) A false and defamatory statement about any person or organisation

(c) Material which is offensive, obscene, criminal, discriminatory, derogatory or

may cause embarrassment to the Trust, its pupils or its parents

(d) Confidential information about the Trust or any employees, pupils or parents (which the employee does not have express authority to disseminate)

(e) Any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or the Trust); or

(f) Material in breach of copyright or other intellectual property rights, or which invades the privacy of any person

9.5 If employees notice any use of social media by other employees in breach of this policy it must be reported immediately to the Chief Executive Officer, Headteacher, Director of Operations . If the concern relates to the Chief Executive Officer, this should be reported to the Chair of the Trust Board.

9.6 If any material is posted on a public platform, regardless of privacy settings, employees have the right to bring this to the Trust's attention and the Trust has the right to investigate the matter further (including whether or not there had been a potential GDPR breach)

10. Reporting and Review

10.1 Where the matter is a safeguarding issue, the Trust should follow the safeguarding procedure and report the matter to the Designated Safeguarding Lead.

10.2 Employees who wish to report other matters related to this policy should do so to the Chief Executive Officer, Headteacher or Director of Operations in the first instance. Concerns relating to the Chief Executive Officer should be reported to the Chair of the Trust Board. Evidence of contravention of the policy must be provided, for example take a 'screen grab' of the relevant page and try to identify the poster.

10.3 If the content is illegal (for example death threats) the police and Trust should be informed as part of the process. The police have powers to request a service provider to disclose data about users. The employer has power to monitor its own IT system under strict regulations.

10.4 Further advice can be sought from the Trusts HR Provider.

11. Equality and Diversity

11.1 The Trust is committed to equality and fairness for all employees and will not discriminate because of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Appendix A Advice on cyberbullying

Advice on cyberbullying

Introduction – What is cyberbullying?

Cyberbullying is the use of technologies by an individual or a group of people to deliberately and repeatedly upset someone else. Cyberbullying is a whole community issue and employees may be victims of cyberbullying from pupils, parents, colleagues or other members of the Trust community.

Such harassment of employees may constitute a criminal offence. It must be taken extremely seriously by the Trust who have a duty to protect the health, safety and wellbeing of employees.

Employee Actions

1. Do not respond directly to the abuser(s) online
2. If possible, capture evidence of the abuse
3. Report the abuse to the Trust
4. Follow Trust policies and procedures
5. Seek medical advice, if physical/mental health is affected
6. Seek additional support from the Trust, if physical/mental health is affected
7. Make a referral to the police in terms of a potential criminal act
8. Notify the service provider

Trust Actions

DfE guidance on cyberbullying states: “Schools should make clear that it is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face.”

The Trust should make sure that pupils, parents, employees and members of the Trust Board are aware of the consequences of cyberbullying and the relevant sanctions that may be applied. It is the duty of every employer under health and safety legislation to ensure, so far as reasonably practicable, the health, safety and welfare at work of all employees. The DfE states that these responsibilities include “seeking to protect staff from cyberbullying, by pupils, parents and other members of staff and supporting them if it happens.”

a. The Trust should ensure that its behaviour policy is applied fully, including use of the full range of sanctions available, up to and including permanent exclusion.

b. Where necessary, the Trust should seek the engagement of parents to support the communication of these expectations and the maintenance of appropriate behaviour standards by pupils.

c. Incidents of harassment, including online abuse of employees by pupils, or parents must be recorded by the Trust as a health and safety incident or dangerous occurrence which has the potential to cause harm.

d. The Trust will respond to an incident in a timely and appropriate manner or support the employee concerned to do so.

e. Where the perpetrator is known to be an adult from the Trust community (e.g., a parent or carer), the Trust should advise them that their behaviour will not be tolerated and remind them of the appropriate ways of raising issues with the Trust.

f. If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, the Trust may consider contacting the local police. Online harassment is a crime.

g. The Trust could obtain screenshots of offensive material for their own records, however, should be cautious about using this material, especially if intending to present the screenshots to parents as evidence. It is important that the Trust does not do anything unlawful with the data, that it is handled confidentially and that consultation with any third party involved takes place before using it.

h. The Trust may approach third party agencies on the employees behalf in order to request that inappropriate material is removed, where possible. Some service providers will not accept complaints lodged by a third party. In cases of mobile phone abuse, where the person being bullied is receiving malicious calls and messages, the account holder will need to contact the provider directly.

i. Where a perpetrator can be identified, there are a number of possible actions open to the Trust or an individual, ranging from requests to the individual to remove the post to claims of defamation or harassment, but the threshold is high to bring a successful claim.

j. Where the perpetrator remains anonymous the Trust will support the employee in cases where it is necessary for the person being bullied to contact the service provider directly.

k. Incidents that occur outside of an employees hours or place of work will also fall under the employer's responsibility if they relate to the employees employment.

l. The Trust should consider and carry out a risk assessment to assess the potential risks that an employee who has been the direct subject of abuse, as well as other employees, may face through their contact with a pupil who has committed online abuse.

m. Given the employer's duty of care to its employees, it may also be necessary in some cases for an employee not to be required to have contact with a pupil who has abused them online in light of the serious distress that such contact could cause.

n. As part of their internet safety procedures, the Trust should ensure that access to social media sites is blocked by default on their own networks.

The UK Safer Internet Centre works with the social networking sites to disseminate their safety and reporting tools.

The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which employees face, such as protecting professional identity, online harassment, or problems affecting young people; for example, cyberbullying or sexting issues.