BUSHBURY HILL PRIMARY SCHOOL

SOCIAL MEDIA POLICY

Document Holder	**Charlotte Underwood**
Date Adopted By Governors	**December 2024**
Review Date	**November 2026**

Working in Partnership

Social Media Policy

ConnectEd Partnership highly recommend the use of this policy. The policy is considered best HR practice, it has been developed in accordance with current employment law and has been negotiated with all recognised professional associations and HR providers across the City of Wolverhampton.

This document was reviewed in October 2024 and the following amendments were made:

A statement has been added regarding the reputation of the School/Academy and preventing potential adverse effects.

A statement regarding employees posting or engaging with anything that brings (or is likely to bring) employees or the school into disrepute, and/or is materially averse to the school's interests, in line with the school code of conduct.

Contents

1. Introduction

1.1 Everything shared on a social networking site could potentially end up in the worldwide public domain and be seen or used by someone you did not intend, even if it appears to be 'private' or is on a closed profile or group."

1.2 The policy has been jointly agreed through consultation and negotiation with Trades Unions/Professional Associations. The policy will be applied fairly and consistently, understood by all users, taking full account of their effect on all areas of activity, satisfying legal requirements and contribute to a productive relationship between the employer, the workforce, and their representatives.

1.3 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 Schools/Academies and Governing/Trust Boards against liability for the actions of their workers.
- Ensure that the reputation of the School/Academy is not compromised via social media and that no one is adversely affected by statements made via social media.
- Help ensure that all employees are aware of their responsibilities regarding 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), Camera Code of Practice (2022), 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 School/Academy and its employees against liability for the actions of its employees, and to help employees draw a line between their private and professional lives by setting out rights, responsibilities and limitations which will help the School/Academy 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/X, Facebook, YouTube, Instagram and LinkedIn, and messaging platforms such as WhatsApp (This list is not exhaustive and the School/Academy recognises that this is a constantly changing landscape).

3.3 This Policy outlines the standards we require employees to observe when using social media, the circumstances in which we will monitor the use of social media and the action we 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 School/Academy 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 School/Academy including: Headteacher, Senior Leadership Team, Teachers, Support Staff, Administrators, Governors, Trustee’s, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as employees in this Policy).

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 School/Academy, its employees, parents, pupils, and any other individual with an association to the School/Academy.

5.2 Employees must not post or engage with anything that brings (or is likely to bring) employees or the school into disrepute, and/or is materially averse to the school's interests, in line with the school code of conduct.

6. Application

6.1 The Policy applies to use of the internet and mobile technologies (such as smart phones/watches/texting/internet and emails/social network sites/blogging and tweeting) whilst outside of the workplace.

6.2 Only the Headteacher or designated staff are permitted to post material on a social media website in the School's/Academy's name. Any breach of this Policy may be subject to disciplinary processes.

7. Responsibilities

7.1 The Headteacher has overall responsibility for the effective operation of this Policy.

7.2 The Headteacher, along with the Governing/Trust Board, is responsible for monitoring and reviewing the operation of this Policy and making recommendations for changes to minimise risks to the School/Academy.

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 the Policy. Breaches of the Policy should be reported to the Headteacher in the first instance.

7.4 Teaching staff must have regard for the Teaching Standards and all staff must recognise professional standards in this respect.

7.5 Questions regarding the content or application of this Policy should be directed to the School's/Academy'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, their place of work or anything else related to work. Raising these issues outside the workplace i.e. via social media, may potentially damage the reputation of the organisation.

7.8 As an employee you must:

- not disclose personal details or identify your geographical location while in work (by disabling access to your 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 you cannot guarantee privacy. If you are a teacher in a School/Academy and a 'friend' with parents, you must not discuss anything relating to the business of the School/Academy and ensure that confidentiality is always maintained.
- 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, [School/Academy], publicise work or private information such as but not limited to telephone numbers, addresses or e-mail addresses.
- not share confidential information or private data relating to knowledge obtained through your employment with the School/Academy.
- ensure that online activities do not interfere with your job, your colleagues or commitments to learners and their parents/carers.
- ensure that if you identify yourself as a School/Academy employee your profile and related content is consistent with how you wish to present yourself with colleagues, learners, and their parents/carers.
- ensure responsibility in reading content carefully before liking a post or posting other emojis to identify your opinion.
- not subject your manager or other colleagues to any use of inappropriate or unwanted political or personal reference either in writing, videos, photographs, text messaging, posting blogs, or email that reveal some form of work-related behaviour (known as cyberbullying - to support

deliberate and hostile attempts to hurt, upset or embarrass another person). In a case of cyberbullying, Headteachers should refer to the Assaults on School/Academy Staff Policy for local conditions of service for School/Academy based employees (teaching and non-teaching). Further guidance on cyberbullying can be found in Appendix 1.

- not compromise the School/Academy and/or colleagues by making adverse, damaging or libellous comments, not using social media to express views (negative or positive) with which the School/Academy would not wish to be connected, which are prejudicial to the best interests of the School/Academy and its employees or contravene the Teacher's Standards - *Teachers' Standards guidance (publishing.service.gov.uk)*.

- be careful if using social networking sites to screen employees as you may run the risk of discriminating against candidates.

- anyone who identifies themselves as School/Academy 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". This may not necessarily prevent the School/Academy from taking disciplinary action, depending on the nature of the comment.

- not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.

- never discuss the School/Academy, 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. This would fall under the Assaults on School/Academy Staff Policy, which staff should refer to.**

8. Policy Breaches

8.1 Employees found to be in breach of this Policy may be subject to disciplinary action, in accordance with The School's'/Academy's agreed/adopted Disciplinary Procedure for teaching and non-teaching employees, 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. Current Arrangements

9.1 In deciding how to respond to work related media usage whilst outside of the workplace, there are three sets of issues to consider:

- Legal
- Ethical
- Practical (including professional behaviour in maintaining confidentiality, not making discriminatory comments, and not sharing private information, during interaction within the social media landscape)

10. Monitoring

10.1 Employers may have legitimate concerns about security that in some way justify a degree of monitoring whilst acknowledging the protection of employee 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 made fully aware of what the employer monitors, how they go about it and why they do so.

10.2 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 School/Academy should invoke the Disciplinary Procedure. Seeking advice from HR your provider is recommended. According to the seriousness of the offence, this could result in action that may ultimately lead to dismissal and/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 and/or the Data Protection Act (GDPR).

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

10.4 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 summary dismissal (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 School/Academy, its pupils or its parents

(d) confidential information about the School/Academy or any employee, pupil or parent (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 School/Academy) or

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

10.5 If employees notice any use of social media by other employees that may be in breach of this Policy, it must be reported immediately to the Headteacher. If the concern relates to the Headteacher, this should be reported to the Chair of the Governing/Trust Board or equivalent.

10.6 If any material is posted on a public platform, regardless of privacy settings, employees have the right to bring this to the School's/Academy's attention and the School/Academy has the right to investigate the matter further (including whether there had been a potential GDPR breach).

11. Reporting and Review

11.1 Where the matter is a safeguarding issue, the School/Academy should follow the safeguarding procedure and report the matter to the Designated Safeguarding Lead.

11.2 Employees who wish to report other matters related to this Policy should do so to the Headteacher in the first instance. 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.

11.3 If the content is illegal (for example death threats) the Police and School/Academy 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.

11.4 Headteachers, in the first instance, should contact their HR provider.

12. Equality and Diversity

The employer 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 1 - Advice on Cyberbullying

Introduction

What is cyberbullying?

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

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

Staff actions

1. Do not respond directly to the abuser(s) online.
2. If possible, capture evidence of the abuse
3. Report the abuse to your employer.
4. Insist that your School/Academy policies and procedures are followed.
5. Seek medical advice, if physical/mental health is affected.
6. Seek additional support from your employer, if physical/mental health is affected.
7. Make a referral to the Police, if your employer has not already done so in terms of a potential criminal act.
8. Notify the service provider, if your employer has not already done so.

School/Academy actions

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

The School/Academy should make sure that pupils, parents, employees, and governors 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 is 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. Schools/Academies should ensure that behaviour policies are applied fully, including use of the full range of sanctions available, up to and including permanent exclusion.

b. Where necessary, Schools/Academies or colleges should seek the engagement of parents to support the communication of these expectations and the maintenance of appropriate behaviour standards by pupils or students.

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

d. The School/Academy 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 School/Academy community (e.g., a parent or carer), the School/Academy should advise them that their behaviour will not be tolerated and remind them of the appropriate ways of raising issues with the School/Academy.

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

g. Schools/Academies could obtain screenshots of offensive material for their own records; however, they should be cautious about using this material, especially if intending to present the screenshots to parents as evidence. It is important that the School/Academy 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 School/Academy may approach third party agencies on the employee’s 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 several possible actions open to the School/Academy 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 School/Academy 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 an employee's 'hours or place of work will also fall under the employer's responsibility if they relate to the employee's employment.

l. The School/Academy 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 or student 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 to prevent contact between an employee and a pupil or student who has abused them online, considering the serious distress that such contact could cause.

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

The UK Safer Internet Centre works with 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.

Professional Associations provide guidance on the personal use of social media via their websites.