



St Peters CofE Primary Academy

Executive Principal: Laura Hopley

Head of School: David Castledine

Chair of Local Academy Committee: Zoe Heath

SOCIAL MEDIA POLICY

St Peter's CofE Academy, Stonnall

Social Media Policy 2022-23

Introduction

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."

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.

It is recognised that Social Media landscapes are likely to be misused and therefore extreme caution should be used at all times.

Background

This policy will:

- Protect Schools and Governing/Trust Boards against liability for the actions of their workers.
- 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.

Purpose of Policy

The aim of this policy is to help protect Schools and employees 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 School prevent any unauthorised comments which might result in creating a legal risk.

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, and LinkedIn (This list is not exhaustive and the school/employer recognise that this is a constantly changing canvas).

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

This policy establishes core standards of behaviour for the use of social media for both personal and professional use. The school 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.

Who is Covered by the Policy

This policy covers all individuals working at all levels and grades within the school including: Headteacher, senior leadership team members, teachers, support staff, administrators, governors, part-time and fixed-term employees, casual and agency staff and volunteers.

The Scope of the policy

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

Application

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

Only the Headteacher or designated persons are permitted to post material on a social media website in the School's name. Any breach of this restriction may be considered as gross misconduct.

Responsibilities

- The Executive Principal has overall responsibility for the effective operation of this policy.
- The Executive Principal, along with the Governing/Trust Board, are responsible for monitoring and reviewing the operation of this policy and making recommendations for changes to minimise risks to the school.
- 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 Headteacher in the first instance.
- Teaching staff must have regard for the Teaching Standards and all staff must recognise professional standards in this respect.
- Questions regarding the content or application of this policy should be directed to the School's HR provider.
- 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.
- 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.

As an employee you must:

- not disclose personal details or identify your geographical location (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 and a 'friend' with parents, you must not discuss anything relating to the business of the school and ensure that confidentiality is maintained at all times.
 - ensure that privacy settings remain unchanged
 - not make references to places of work, school, publicise work or private - telephone numbers, addresses or e-mail addresses
 - not share private data relating to knowledge obtained through your employment with the School.
 - not disclose any confidential information in relation to your employment
 - 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 employee your profile and related content is consistent with how you wish to present yourself with colleagues, learners and their parents/carers.
 - 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 Cyber bullying - to support deliberate and hostile attempts to hurt, upset or embarrass another person). In a case of Cyber bullying, Headteachers should refer to the Anti-bullying and Harassment Policy for Local conditions of service for School based employees (teaching and non-teaching) in schools.
- not compromise the school/employer and/or colleagues by making adverse, damaging or libellous comments, using social media to express views (negative or positive) with which the School would not wish to be connected, which are prejudicial to the best interests of the school and its employees.

- 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 employees 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 school, pupils or parents/carers on social media
- be aware of discussing topics that may be inflammatory.

Policy Breaches

Employees found to be in breach of this policy may be subject to disciplinary action, in accordance with the Local Agreement Disciplinary Procedure for teaching and nonteaching staff in schools, with possible sanctions up to and including dismissal.

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

Current Arrangements

In deciding how to respond to work related media usage whilst outside of the workplace both public and in-house, 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)

Monitoring

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 employers monitor, how they go about it and why they do so.

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 should invoke the Disciplinary procedure. According to the seriousness of the offence, this could result in action that may ultimately lead to dismissal. 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).

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

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, its pupils or its parents;
- (d) confidential information about us or any of our staff, pupils or parents (which you do not have express authority to disseminate);

(e) any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or

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

If employees notice any use of social media by other members of staff in breach of this policy it should be reported immediately to the Headteacher or Chair of the Governing/Trust Board or equivalent.

Reporting and Review

Staff who wish to report a matter related to this policy should do so to the Executive Principal 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.

If the content is illegal (for example death threats) the police should be contacted. They have powers to request a service provider to disclose data about users.

Headteachers in the first instance should contact their Schools HR Consultant.

Date of issue: **September 2022**

Review date: **September 2023**