St Paul's CE Primary School

Social Networking

Policy

2026-2027

Agreed by Governing Body on:	**20 May 2026**
Policy review date:	**May 2027**

Based on B&H model policy

Model Social Networking Policy for BHCC Schools

1. Introduction

1.1 The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

1.2 Whilst the widespread availability and use of social networking applications brings opportunities to engage and communicate with audiences in new and exciting ways, it is important to ensure that we balance this not only with our legal responsibilities to safeguard and protect our children and staff but also with the need to safeguard the school's image and reputation.

1.3 *The school E Safety Policy which includes a wider range of information on home and school ICT use, security & safeguarding issues (including how all school staff will be made aware of relevant issues and whom they should contact within the school if any concerns arise) should be read alongside this policy. See also Para. 9 below.*

2. Purpose

2.1 The purpose of this policy is to:

- support safer working practice by setting out the key principles and expected standards of behaviour when using social networking media
- ensure all children are safeguarded
- ensure the reputation of the school (its staff, pupils and governors at the school) are not damaged or compromised
- ensure that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the School
- minimise the risk of misplaced or malicious allegations being made against those who work with pupils
- reduce the incidence of positions of trust being abused or misused
- ensure the school, its governors and staff are not exposed to legal risks.

3. Scope

3.1 This policy applies to the governing body, all teaching and other staff, whether employed by Brighton & Hove City Council or employed directly by the school, individual governors, external contractors

providing services on behalf of the school or the City Council, teacher trainees and other trainees, supply staff, agency workers, volunteers and other individuals who work for, or provide services on behalf of, the school. These individuals are collectively referred to as 'staff members' in this policy.

3.2 This policy cannot cover all eventualities and, therefore, staff members should consult the Headteacher if they are in any way unsure about what is and isn't acceptable use of social media.

4. Legal Framework

4.1 St Paul's CE Primary School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of the law and professional codes of conduct.

4.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or Brighton & Hove City Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information.

4.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media.

4.4 St Paul's CE Primary School and Brighton & Hove City Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the school or the County Council liable to the injured party.

5. Definition of Social Media

5.1 Social media is the term commonly used for websites which allow people to interact with each other in some way by sharing information, opinions, knowledge and interests. Social networking websites such as

Facebook, Bebo and MySpace are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, mircoblogs such as *Twitter*, chatrooms, forums, video and audio podcasts, open access online encyclopaedias such as *Wikipedia, message boards, photo document,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*.

5.2 This definition of social media is not exhaustive. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media. However, the principles set out in this policy must be followed irrespective of the medium.

5.3 For the purpose of this policy, the term social media also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

6. Principles - Social Media Practice

6.1 Staff members need to be aware that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and will be shared.

6.2 Staff members must be conscious at all times of the need to keep their personal and professional lives separate and to always maintain appropriate professional boundaries.

6.3 Staff members are responsible for their own actions and conduct and should avoid behaviour which might be misinterpreted by others or which could put them in a position where there is a conflict between their work for the school or Brighton & Hove City Council and their personal interests.

6.4 They must use social media in a professional, responsible and respectful way and must comply with the law, including equalities legislation, in their on-line communications.

6.5 Staff members must not engage in activities involving social media which might bring the school or the Council into disrepute.

6.6 They must not represent their personal views as those of the school or the Council on any social medium.

6.7 They must not discuss personal information about pupils, their family members, school or Council staff or any other professionals or organisations they interact with as part of their job on social media.

6.8 They must not name or otherwise identify pupils, former pupils or their parents, family members, colleagues etc in social media conversations.

6.9 They must not use social media or the internet in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about pupils, their family members, colleagues, other professionals, other organisations, the school or the Council.

6.10 They must not browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

6.11 They must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

7. Personal Use of Social Media

7.1 Staff members need to be aware of the dangers of putting personal information such as addresses, home and mobile phone numbers, email addresses etc. onto social networking sites.

7.2 Staff members should ensure that they set the privacy levels of their personal sites at the maximum and opt out of public listings on social networking sites to protect their privacy.

7.3 Staff members should keep their passwords confidential, change them often and be careful about what is posted online. It is a good idea to use a separate email address just for social networking so that any other contact details are not disclosed.

7.4 Staff members should not identify themselves as employees of the school or Brighton & Hove City Council or service providers for the school or the City Council **in their personal webspace**. This is to prevent information on these sites being linked with the school or the Council. Where possible it may be useful to add a disclaimer such as "these are my own views and opinions and not those of my employer"

7.5 Taking the steps outlined in paragraphs 7.2 to 7.4 will avoid the potential for staff members to be contacted by pupils or their families or friends outside of the school environment and will reduce the chances of them becoming victims of identity theft.

7.6 All staff members should try to regularly review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This should be suggested to new staff when they join the school. It is also good practice to close old accounts as they may contain personal information about you.

7.7 Staff members must not give their personal contact details including details of any blogs or personal social media sites or other websites to pupils or former pupils. It is also important to be aware that ex pupils may still have siblings in the school. Please refer to your schools own e-safety policy for more specific information. Please also see point 2.1 of this policy.

7.8 Staff members must not have contact through any personal social medium with any pupil, whether from this or any other school, unless the pupil is a family member or it is through school approved sites as part of official collaborative work. See point 7.11 below.

7.9 The school does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

7.10 It is strongly recommended that staff members do not have any contact with pupils' family members through personal social media. Please see point 6.1 & 6.2 above.

7.11 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites.

7.12 Staff members must not establish, or seek to establish, social contact via social media/other communication technologies with pupils or ex-pupils and must never "friend" a pupil or ex-pupil through social media. These actions could be construed as being part of a "grooming process" in the context of sexual offending. This should be echoed in the school's policy also. In the case of some social networking sites it is possible to be 'followed' by a pupil without your consent. If this is the case, then your school should be informed and the pupil 'follower' deleted.

7.13 Staff members must never use or access pupils' social networking sites.

7.14 Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. If they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official school site or follow the school's own policy.

7.15 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss or publish inappropriate information. Staff members must therefore make sure that they do not publish

confidential information that they have access to as part of their employment on their personal webspace. This includes personal information about pupils, their family members, colleagues, Brighton & Hove City Council staff and other parties as well as school or City Council related information. This requirement continues after they have left employment.

7.16 Similarly, photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school or City Council uniforms or clothing with school or City Council logos or images identifying sensitive school or Council premises (e.g. care homes, secure units) must not be published on **personal webspace**.

7.17 The school or Council's corporate, service or team logos or brands must also not be used or published on personal webspace.

7.18 Staff members must not use school or City Council email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

7.19 Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

7.20 Staff members are advised to be cautious about inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and this may make it difficult to maintain professional relationships or embarrassing if too much personal information is known in the work place.

7.21 On leaving St Paul's CE Primary School's service, staff members must not contact St Paul's CE Primary School's pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

8. Breaches of the Policy

8.1 Any breach of this policy may lead to disciplinary action, including the possibility of dismissal being taken against the staff member/s involved in line with St Paul's CE Primary School or Brighton & Hove City Council's Disciplinary Procedure.

8.2 Contracted providers of St Paul's CE Primary School or Brighton & Hove City Council services must inform the Headteacher immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation

of the school and the Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

9. Links to other Policies/Standards

9.1 This policy should be read in conjunction with the following policies:

- School E-Safety policy or equivalent
- School Bullying policy or equivalent
- School Data Security policy or equivalent
- Staff Acceptable Use (of ICT) policy
- School Code of Conduct
- Child Protection/Safeguarding policies

Teacher's Standards 2012
https://www.education.gov.uk/publications/eOrderingDownload/teachers%20standards.pdf

10. Further Information

Kent e-Safety Policies, Information and Guidance

http://www.kenttrustweb.org.uk//Children/safeguards_esafety.cfm

UK Safer Internet Centre Professional Helpline
http://www.swgfl.org.uk/News/Content/News-Articles/Professionals-Online-Safety-Helpline

NASUWT Social Networking Guidance for Members
http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking/NASUWT_007513

NUT Social Media Guidance April 2012
http://bit.ly/XL5aME

ATL Advice
http://bit.ly/YOpxfd

Signed ……Chair of Governors.

Date:……..

Signed …….Headteacher.

Date:……..