Highcliffe St Mark Primary & Fledglings Pre-School

Social Networking Policy

DSL Gavin Withey
Deputy DSLs Claire Barker, Jacqui Fuller, Emma Stansbie, Darren Whittaker, Laura Simmons, Pippa Pandit
Safeguarding Governor Lisa Caola

Reviewed (date)	September 2026
Reviewed by (name)	Gavin Withey
Approved by Governors (if applicable)	
Review due (date)	September 2027

Introduction

Aims

This document sets out our school policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for school staff in many ways. Highcliffe St Mark Primary School recognises and embraces the numerous benefits and opportunities that social media offers. While staff are encouraged to engage, collaborate and innovate through social media, they should always be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation. This document aims to:

- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice and encourage good practice, to protect the school and its employees, and to promote the effective use of social media as part of the school's activities
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils which can impact on the wellbeing of staff, pupils and the reputation of the school
- Reduce the incidence of positions of trust being abused or misused
- Enable school staff to enjoy the benefits of social networking while understanding the standards of conduct expected by the school

Purpose of the policy

- 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 in school will always advise the Headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from the Schools HR team 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 listed at appendix A.
- This policy covers personal and professional use of social media including personal communications via social media accounts which are likely to have a negative impact on professional standards or the school's reputation.
- This document applies to all staff who work in Highcliffe St Mark Primary School as adopted by the governing body. This includes teachers, support staff, supply staff, governors, contractors and volunteers.
- Any adult whose work brings them into contact with pupils should follow it.

- References to staff should be taken to apply to all the above groups of people in school. Reference to pupils means all pupils at the school.
- This policy should not be used to address issues where other policies and procedures exist to deal with them. For example, any alleged misconduct which falls within the scope of the management of allegations policy requires the school to comply with additional child protection requirements as set out in that policy.

Roles, responsibilities and procedure

This document does not replace or take priority over advice given by HR, BCP safeguarding team or the school's staff and volunteer code of conduct, dealing with allegations of abuse other policies issued around safeguarding (email, ICT and data protection policies), but is intended to both supplement and complement any such documents. This guidance has been agreed with the trade unions.

Employees working in our school should:

- be responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions
- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media
- work and be seen to work, in an open and transparent way
- continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document and other related policies
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they post on a social networking site is something that they want pupils, colleagues, other employees or future employees to read.

The Leadership Team and Governing Body are responsible for:

- addressing any concerns and/or questions employees may have on the use of social media
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

Safer Social Media Practice in Schools

What is social media?

For the purpose of this document the terminology Social Media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Instagram and YouTube. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.

Overview and expectations

- All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or public in general and all of those with whom they work in line with the school's code of conduct. Adults in contact with pupils 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 school staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken.

Safer online behaviour

- Managing personal information effectively makes it far less likely that information will be misused. Staff should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, staff using social media should conduct themselves with professionalism and respect.
- 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 pupils 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.
- Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, the school, their colleagues, pupils or members of the public.
- 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, pupils or other individuals connected with the school or another school or BCP Council could result in formal action being taken against them.
- Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications. They should not upload content to social media sites that amounts to bullying, unlawful discrimination, harassment or victimisation.
- Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or BCP Council into disrepute.
- Staff should not upload content to social media which contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips.

- 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 a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.
- Staff should be careful not to upload content which breaches copyright law.

Protection of personal information

- Staff should ensure that they do not use school computing equipment for personal use, e.g. computers or IPADs.
- Staff should keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.
- Staff should never share their work log-ins or passwords with other people.
- Staff should not give their personal e-mail addresses to pupils or parents.

Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people. Any content or online activity which raises a safeguarding concern must be reported to the DSL at school or the Headteacher if it involves an allegation against a member of school staff. In the event that the safeguarding concern is regarding the Headteacher, the Chair of Governors should be consulted.

- Any online concerns should be reported as soon as identified as urgent steps may need to be taken.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Social contact

- Staff should not establish or seek to establish social contact via social media / other communication technologies with pupils for the purpose of securing a friendship or to pursue or strengthen a relationship.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.
- There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

Cyberbullying

- Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
- Staff should never engage with cyberbullying incident. If in the course of your employment at our school you discover a website containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken

and/or are being used without your permission, you should immediately report this to a senior leader.

- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of the site should be recorded.

Action by Headteacher and/or Governing Body: inappropriate use of social media

- Following a report of inappropriate use of social media, the Headteacher will conduct a prompt investigation.
- If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the school's behaviour policy.
- The Headteacher, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, i.e. within 24 hours. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.
- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the Headteacher will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.
- If the material is threatening and/or intimidating, the Headteacher will, with the member of staff's consent, report the matter to the police.
- The member of staff will be offered full support and appropriate stress counselling.

Breaches of this policy

Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the school's bullying or disciplinary procedure. The member of staff will be expected to co-operate with the school's investigation which may involve:

- handing over relevant passwords and login details;
- printing a copy or obtaining a screenshot of the alleged unacceptable content;
- determining that the responsibility or source of the content was in fact the member of staff.

The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school or the individuals concerned. Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure. If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee. Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

Review of policy

Due to the ever changing nature of information and communication technologies, it is best practice that this policy be reviewed annually and if necessary more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Legislation

Acceptable use of social networking must comply with UK law. In applying this policy, the school/trust will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium. When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment. Staff should use discretion and common sense when engaging in online communication. There are some general rules and best practice in the appendix which staff may find helpful.

Appendices

Appendix A – Responsible use of social media – guidance for staff

Remember that anything you post online is not really private. Below are some common-sense guidelines and recommendations that staff are advised to follow to ensure responsible and safe use of social media.

- Do not add pupils as friends or contacts in your social media accounts.
- Follow this social media policy.
- Always maintain professional boundaries. Do not engage in discussion with pupils online unless through official school accounts.
- Think about the potential risks: professional boundaries of adding parents to your private social media accounts (refer to policy).
- Consider using an alternative name on sites like Facebook to make it harder for pupils to find you. For example, some members use their partner's surname online but their own surname in school.
- Never post anything that is offensive or aggressive, even if you are very angry or upset. It can easily be taken out of context.
- Remember humour is relative. For example, posting images and/or text about a recent stag or hen night may be deemed inappropriate. Likewise, a few 'light-hearted' comments and/or images about colleagues or students may not be perceived as such by either subject(s) of the humour or the employer. The guiding rule is: if in doubt, don't post it.
- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.
- If you are tagged in something, for example – Facebook, that you consider inappropriate, use the remove tag feature to untag yourself (for details on how to do this, refer to the sitehelp centre).
- Be cautious of accepting 'friend requests' from people you do not really know. Simply being a 'friend' of a friend does not mean that they should automatically be given access to your information.
- Review your profile information and settings on Facebook, Twitter and other sites to ensure it is appropriate as it may be accessed by others such as colleagues, pupils, parents and potential employers.
- Check your privacy and security settings regularly, and keep your date of birth and home address to yourself. Identity theft is a growing crime and this kind of information could be used to gain access to your bank or credit card account.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.
- Never post any information which can be used to identify a pupil.
- Do not use social media in any way to attack or abuse colleagues or air any other internal grievances.
- Do not post derogatory, defamatory, offensive, harassing or discriminatory content.
- Do not engage in any conduct (using personal insults, obscenities) which would not be acceptable in the workplace.
- Do not use social media to 'whistle blow' – raise concerns through the proper channels which would entitle you to legal protection (Public Interest Disclosure Act 1998)

VERSION	DATE	REVIEWER	COMMENT
1	September 25	GW	Change made to School name and DSL's