

Social Media Policy

Date: Autumn 2019, 2022 and 2025

This document should be read in conjunction with information contained in the Acceptable Use of ICT Policy, the Online Safety Policy, the Mobile Phone Policy, the Online Learning Policy, Data Protection Policy and the AI Policy.

Where staff have concerns about online safety, these should be raised with the Head Teacher. Advice can also be sought from professional associations.

Signposting:
https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools
https://nationalonlinesafety.com/guides

Risks

The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- cyber bullying by pupils/students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff or pupils/students
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the school;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

Social media and social networking sites play an important role in the lives of many people. We recognise that sites bring risks, but equally there are many benefits to be reaped. This gives clarity to the way in which social media/mobile phones are to be used by pupils, social media/mobile phones are to be used by pupils, governors, visitors, parent helpers and school staff at Ferndale Primary School. It will also provide guidance for parents.

There are four key areas:

A. The use of social networking sites by pupils within school
B. Use of social networking by staff in a personal capacity
C. Comments posted by parents/carers
D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school

The school's Acceptable Use Policy (AUP) outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Such sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate.

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two. Others have higher age restrictions. If it is found out in school that a child has been using social media, parents will be informed to ensure they are aware. The risk of exploitation and radicalisation is increased by inappropriate use of social media and children are taught about such dangers as part of our Online Safety curriculum. Children are also taught about healthy relationships as part of PSHE.

Ferndale uses the parent app; reach more parents by weduc. The news feature from this app transfers to our school's website through the use of a 'dummy' Facebook account.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never add** pupils as 'friends' into their personal accounts (including **past** pupils under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Personal social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.

- Staff members must report any safeguarding issues they become aware of.
- Material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party.
- The tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner.
- If used with pupils/students, staff must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- Staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.
- Staff have a Code of Conduct that they are expected to sign to say they have read and understood.

Personal use of internet and social media

The school's Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for private use and access can be withdrawn at any time. Where staff members are permitted access via the school's Internet connection:

- the school is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- staff wishing to spend significant time outside of their own normal working hours using the Internet – e.g. for study purposes must obtain prior approval;
- inappropriate or excessive use may result in disciplinary action and/or removal of Internet facilities;
- the school will monitor Internet and email use by electronic means (SENSO), and staff cannot expect privacy when using the school devices;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only and school's disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a colleague, or some other legitimate and objective complaint or incident;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff concerned about this should refrain from using the Internet for private matters;
- staff members may not download software from any source without approval.

- staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Head Teacher

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include admission paperwork, the website, parent app, Arbor, school portal, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion.
Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event. Parents should make complaints through official school channels rather than posting them on social networking sites.
Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

Senior Leadership responsibility in relation to Bullying and Harassment

The school will take reasonable steps to provide a safe working environment free from bullying and harassment.
For this reason, it is essential that the Senior Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, X, or by any other means.

If a Senior Leader is made aware of such an allegation, the Senior Leadership Team will deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

Staff should preserve all evidence by not deleting emails, excluding spam emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Senior Leadership Team should consider advising the employee that they should inform the police.

In the case of inappropriate use of social networking by parents about the school, the Governing Body or member of staff will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Headteachers)

Peer protection:

We recognise that children can abuse other children. This is referred to as peer on peer abuse and can take many forms that may be demonstrated through poor behaviour in the school setting; bullying (including cyber-bullying); sexual violence and sexual harassment (online or via texts); sexting and initiating/hazing type violence and rituals.

We aim to prevent this through our PSHME curriculum, mentoring sessions and through staff awareness. However, should an incident arise, it will be investigated fully by the class teacher in the

first instance. Should peer on peer abuse be suspected, this will be escalated to the DSL or deputy DSL in their absence.

Sanctions will be issued in line with this policy, alongside the Safeguarding Policy and relevant outside agencies may be informed. Support for the victim will reflect the circumstances of the incident, but could be offered internally through the school's own pastoral processes or through external agencies.

The document Keeping Children Safe in Education is issued to schools detailing statutory guidance, placing a duty on schools to promote the welfare of children. This social media policy complies with the government guidance stated in the KCSIE 2024 document and will change as necessary to subsequent versions as appropriate.