Social Media Policy

Person(s) Responsible:	Headteacher
Formally adopted by the Governing Body:	March 2024
Review date:	March 2025

This policy also applies to the Early Years Foundation Stage (EYFS)

Contents

1. Rationale and aims

Rationale

The governors, staff and School Council of Biggin Hill Primary School recognise that social media sites are now regularly used. This type of media allows people to communicate in ways that were not previously possible and there are numerous benefits and opportunities to doing so. The majority of stakeholders use social media in a positive way and responsible way. However they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Aims

- To inform all members of our school community about the appropriate use of social media at our school
- To outline the procedures and processes of this policy
- Promote, and set an example for, safe and responsible social media use
- Set clear guidelines for the use of social media for pupils, staff, parents/carers and volunteers
- Support the school's other policies, especially those related to child protection and behaviour.

2. Roles and responsibilities

All staff (including teachers, support staff, and supply staff) are responsible for enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The head teacher is responsible for monitoring the policy, reviewing it, and holding staff and pupils accountable for its implementation.

3. Use of official school social media

The school's official social media is X (formerly Twitter). The X username is @BigginHillPS

These accounts are managed by authorised staff members. Staff members who have not been authorised by SLT to manage, or post to, the account, must not access, or attempt to access, these accounts.

If you have suggestions for something you'd like to appear on our school social media channel, please speak to SLT.

3.1 X (formerly Twitter)

The school posts on X:

- Alerts about changes (e.g. changes to procedures, severe weather updates, staffing changes)
- Reminders (e.g. approaching deadlines, events or class activities, reminders about policies/procedures)
- Advertisements for school events or activities
- Job vacancies or requests for volunteers
- Links to newsletters, guidance and factsheets for parents and carers
- Achievements of pupils and staff
- Photos or posts about school trips, events and activities
- Seasonal greetings and messages about religious festivals
- Invitations to provide feedback

The school **will not** post on X:

- Names and photos of individuals (unless they have given consent)
- Harmful or abusive comments
- Messages to specific people
- Political statements
- Advertisements for businesses unless directly related to the school
- Links to staff members' personal accounts

3.2 Moderation

Staff responsible for our social media accounts will delete as soon as reasonably possible:

- Abusive, racist, sexist, homophobic or inflammatory comments
- Comments we consider to be spam
- Personal information, such as telephone numbers, address details, etc.
- Posts that advertise commercial activity or ask for donations

Every reasonable effort will be taken to politely address concerns or behaviour of individual users, following the school's complaints policy. If users are repeatedly abusive or inappropriate, they will be blocked.

Staff responsible for our social media accounts will also ensure that all content shared on social media platforms is age appropriate for the school community.

3.3 Following other social media users

The school will only 'follow' X (formerly Twitter) users with a non-commercial interest – being 'followed' by us doesn't imply endorsement of any kind

4. Use of social media by staff

Staff members are strongly encouraged not to identify themselves as staff members of their School in their personal social media platforms. This is to prevent information on these sites from being linked with the school or Academy Trust and to safeguard the privacy of staff members. This does not include professional networking sites.

Staff should not have contact through any social medium with any student from the named School or any other school. Staff should decline 'friend requests' from students they receive in their personal social media accounts.

In cases where staff are also parents/carers connected to the school, they are advised to use professional judgement (in reference to child protection and safeguarding policies) when

communicating with children or young people also connected to the school community. Staff should only accept friend requests/communicate (when there is a genuine need) with others linked to the school community. This relationship should stand up to scrutiny from a professional perspective and should be appropriate. If a concern of safeguarding arises, this should be reported to the designated safeguarding lead in accordance with the safeguarding policy.

Photographs, videos or any images of pupils or students should not be published on personal social media platforms without prior permission of parents/carers and the school. Permission should be gained through existing school procedures.

School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media unless pre-approved by school leadership.

Staff are strongly advised to ensure that they set up and regularly review the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

Staff should also select carefully their social media profile picture as it is an extension to their professional image online. Social media should not be used for work related communication. Communication should be through school email or contact details held by the school. Any misuse or abuse of social media must be reported to the Head Teacher as soon as noticed, especially when concerning a pupil, parent/guardian or employee.

Members of staff **must not** post content online which is damaging to the school or any of its staff or pupils. Teachers or members of staff must not post any information which could identify a pupil, class or the school. Members of staff should not post anonymously or under an alias to evade the guidance given in this policy. Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.

5. Use of social media by pupils

- The school's Acceptable Use Policy (AUP) outlines the rules for using IT in school and these rules therefore apply to the use of social networking sites.
- Photographs, videos or any image of pupils, staff or any member of our school community must not be published on a personal or public web space without prior permission from the school.

- Pupils should not make inappropriate comments (including in private messages) about the school, teachers or other children.
- Social network sites should never be accessed within school.
- Failure to follow these guidelines may result in disciplinary action.
- Pupils should be taught as part of their e-safety lessons how to report abuse and inappropriate content.
- Biggin Hill Primary does not support pupils signing up to social media sites that have an age restriction above the pupil's age.

6. Use of social media by parents, carers and guardians

Parents/Carers 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. Personal phones and cameras are not allowed to be used by parents/carers while they are on school premises unless specific permission is granted.

All communication must be made through official school channels including any complaints. Where a parent has a concern, this must be made through the appropriate channels by speaking to the class teacher, the Headteacher or Chair of Governors so they can be dealt with fairly, appropriately and effectively for all concerned (See Complaints Policy).

Parents/Carers should not post malicious or fictitious comments on social networking sites about any member of the school community. Legal advice may be sought and/or police may be contacted should this be the case. Malicious or inappropriate comments will be reported and may result in accounts being removed. Fictitious and defamatory comments may also result in legal action. Action will also be taken if any inappropriate comments are made in which a member of the school community can be identified from the content of the comment.

We expect parents/carers to follow the above social media guidelines when using class WhatsApp groups.

Parents/Carers should also ensure that their children are not using social networking/internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online.

7. Cyber Bullying

Cyberbullying is making use of information and communications technology, particularly mobile phones and the internet, to deliberately undermine, humiliate or otherwise cause distress to the person on the receiving end. At Biggin Hill Primary School, cyber bullying is taken seriously and incidents of cyber bullying will be dealt with and reported along the same chain as the Anti-Bullying Policy.

According to the anti-bullying organisation, Bullying UK, cyberbullying can take place in many different shapes and forms. These include:

- Harassment - which includes the sending of nasty, offensive, insulting, derogatory and abusive messages, photos or videos on social media.
- Denigration - this involves someone sending information about others that is false, distorted and unfounded for the purpose of damaging their reputation, character, or personal and/or professional status.
- Flaming - this is when extreme and offensive language is used to create conflict and arguments online.
- Impersonation - this is when your personal identity and information (name, photos, and personal details) are cloned and stolen in order to make fake social media accounts.
- Outing and trickery - this is when someone may share personal information, photos, or videos that are used against them.
- Cyber-stalking - this is an illegal offence and includes sending threats, intimidation and engaging in other online activity that makes others feel unsafe online or in real life.
- Exclusion - this involves intentionally leaving someone out of your social media networking circles.

Staff should not personally engage with cyberbullying incidents and should immediately report incidents to the Head Teacher. If a member of staff is the victim (receives any threats, abuse or harassment from members of the public through their use of social media), they should keep any records of the abuse and if appropriate, screen prints of messages or web pages with time, date and address of the site. Staff must report such incidents using the school's procedures.

Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures.

Staff members and pupils 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, other pupils or parents/carers, can find its way into the public domain even when not intended.

Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content. If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions. If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.

If cyberbullying does take place involving a child the school will follow its procedure outlined in the anti-bullying policy.

As part of our on-going commitment to the prevention of cyberbullying, regular education and discussion about e-safety will take place as part of Computing and Personal, Social, Health and Education (PSHE).

8. Monitoring arrangements

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, for legitimate business purposes. This includes ascertaining and demonstrating that expected standards are being met by those using the systems, and for the detection and investigation of unauthorised use of the systems (including where this is necessary to prevent or detect crime).

The DSL will log behaviour and safeguarding issues related to online safety.

All staff have responsibility for reporting concerns relating to online safety using the school's procedures.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board.

9. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Online safety policy
- Mobile Phone Policy
- Complaints procedure
- Whistleblowing Policy
- GDPR Policy

All staff must adhere to, and apply, the safe use of social media within this policy in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.