



Social Media Policy

Policy Approved	April 2025
Review Date	April 2026
Responsible Staff	R. Flanders
Governor	A. Avery

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Definitions
4. Data protection principles
5. Social media use – staff
6. Social media use – pupils and parents
7. Blocked content
8. Cyber bullying
9. Training
10. Monitoring and review

Statement of intent

Hoole Church of England Primary School understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and pupils in support of the school's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

1. Legal framework

1.1. This policy has due regard to legislation and guidance including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- DfE 'Data protection: a tool kit for schools'
The Data Protection Act

1.2. This policy will be implemented in accordance with the following school policies and documents:

- Staff handbook
- E-Safety Policy
- Confidentiality Policy
- GDPR policy
- Complaints Policy
- Anti-Bullying Policy
- Allegations of Abuse Against Staff Policy
- Disciplinary Policy
- Grievance Policy

2. Roles and responsibilities

2.1. The headteacher is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents/carers and pupils are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.

- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the school ICT technician and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with the GDPR.

2.2. Staff members are responsible for:

- Adhering to the principles outlined in this policy, the staff handbook and other related policies/documents including the Whistleblowing Policy and the Confidentiality Policy.
- Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff, pupils or parents/carers to the headteacher immediately.

2.3. Parents/carers are responsible for:

- Adhering to the principles outlined in this policy and the Home School Agreement.
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.
- Attending e-safety meetings held by the school wherever possible.

2.4. Pupils are responsible for:

- Adhering to the principles outlined in this policy and the Home School Agreement.
- Ensuring they understand how to use social media appropriately and stay safe online.

3. Definitions

3.1. For the purpose of this policy, the school defines “**social media**” as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- ‘Micro-blogging’ applications, such as Twitter

- 3.2. For the purpose of this policy, “**cyber bullying**” is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.
- 3.3. For the purpose of this policy, “**members of the school community**” are defined as any teacher, member of support staff, pupil, parent/carer of a pupil, governor or ex-pupil.

4. Data protection principles

- 4.1. The school will obtain consent from pupils and parents/carers at the beginning of each academic year using the Images and Videos Parental Consent Form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the entire academic year.
- 4.2. A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The Data Protection Officer (DPO) is responsible for ensuring this consent record remains up to date.
- 4.3. For the purpose of section 4.1, where a pupil is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the child.
- 4.4. Parents/carers and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing.
- 4.5. Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided.
- 4.6. Where parents/carers or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents'/carers' and pupils' requirements following this.
- 4.7. In line with section 4.5, wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.
- 4.8. The school will only post images and videos of pupils for whom consent has been received.

- 4.9. Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the school ICT technician for use.
- 4.10. The school will not post pupils' personal details on social media platforms.
- 4.11. Pupils' full names will never be used alongside any videos or images in which they are present.
- 4.12. Only appropriate images and videos of pupils will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- 4.13. When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.
- 4.14. Before posting on social media, staff will:
 - Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
 - Ensure that there is no additional identifying information relating to a pupil.
- 4.15. Any breaches of the data protection principles will be handled in accordance with the school's GDPR Policy.
- 4.16. Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents/carers are not permitted to post any imagery or videos on personal accounts.

5. Social media use – staff

School accounts

- 5.1. Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements.
- 5.2. Staff will not post any content online which is damaging to the school or any of its staff or pupils.

Personal accounts

- 5.3. Staff members will not access social media platforms whilst on school premises.
- 5.4. Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the headteacher.

- 5.5. Staff members are permitted to use social media during break times.
- 5.6. Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the headteacher, and once the school ICT technician has ensured the necessary network security controls are applied.
- 5.7. Staff will avoid using social media in front of pupils.
- 5.8. Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.
- 5.9. If pupils or parents attempt to "friend" a staff member they will report this to the headteacher.
- 5.10. Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels.
- 5.11. Staff members will ensure the necessary privacy controls are applied to personal accounts.
- 5.12. Staff members will avoid identifying themselves as an employee of Hoole Church of England Primary School on their personal social media accounts.
- 5.13. No staff member will post any content online that is damaging to the school or any of its staff or pupils.
- 5.14. Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- 5.15. Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.
- 5.16. Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- 5.17. 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.
- 5.18. Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- 5.19. Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

6. Social media use – pupils and parents/carers

- 6.1. Pupils will not access social media, unless it is part of a curriculum activity.
- 6.2. Pupils and parents/carers will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts. Pupils and parents/carers are only permitted to be affiliates of school social media accounts.
- 6.3. Where a pupil or parent/carer attempts to “friend” a staff member on their personal account, it will be reported to the headteacher.
- 6.4. Pupils and parents/carers will not post any content online which is damaging to the school or any of its staff or pupils.
- 6.5. Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil’s age.
- 6.6. If inappropriate content is accessed online on school premises, it will be reported to a teacher.
- 6.7. Pupils are not permitted to use the school’s WiFi network to access any social media platforms unless prior permission has been sought from the headteacher, and the school ICT technician has ensured appropriate network security measures are applied.
- 6.8. Parents/carers are not permitted to use the school’s WiFi network to access any social media platforms on personal devices.
- 6.9. Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.

7. Blocked content

- 7.1. In accordance with the school’s GDPR Policy, the school ICT technician installs firewalls on the school’s network to prevent access to certain websites. The following social media websites are not accessible on the school’s network:
 - Twitter
 - Facebook
 - Instagram
- 7.2. Attempts made to circumvent the network’s firewalls will result in a ban from using school computing equipment, other than with close supervision.

- 7.3. Inappropriate content accessed on the school's computers will be reported to the ICT Technician via the school ICT Leader so that the site can be blocked.
- 7.4. The headteacher retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

8. Cyber bullying

- 8.1. Cyber bullying incidents are taken seriously at Hoole Church of England Primary School. Any reports of cyber bullying on social media platforms by pupils will be handled in accordance with the Anti-Bullying Policy.
- 8.2. Allegations of cyber bullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.
- 8.3. Staff members will not respond or retaliate to cyber bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the headteacher.
- 8.4. Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.
- 8.5. Where the perpetrator is a current pupil or colleague, most incidents can be handled through the school's own disciplinary procedures.
- 8.6. Where the perpetrator is an adult, in nearly all cases, a member of the SLT will invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- 8.7. 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.
- 8.8. If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school will consider whether the police should be contacted.
- 8.9. As part of the school's ongoing commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

9. Training

- 9.1. At Hoole Church of England Primary School, we recognise that early intervention can protect pupils who may be at risk of cyber bullying or

negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.

- 9.2. Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.
- 9.3. Teachers and support staff will receive ongoing training as part of their development.
- 9.4. Pupils will be educated about e-safety and appropriate social media use on a termly basis through a variety of mediums, including: assemblies, PSHE lessons and cross-curricular links.
- 9.5. Pupils will be provided with material to reinforce their knowledge via regular sessions focused on e-safety organised by the ICT Leader.
- 9.6. Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

10. Monitoring and review

- 10.1. This policy will be reviewed on an annual basis by the headteacher, in conjunction with the school ICT Leader and DPO.
- 10.2. The next scheduled review date for this policy is April 2026.
- 10.3. Any changes made to this policy will be communicated to all staff, pupils and parents.

