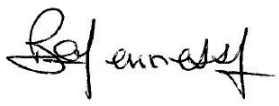
Huntington

Community Primary School

Social Media Policy

Signed by:

Headteacher Date: 04.03.21



Chair of Governors Date: 04.03.21

Next review Spring 2024

Contents:

Statement of intent

Huntington Community 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 ethos, aims 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 online bullying and potentially career-damaging behaviour.
- Providing online safety training for pupils and 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 (2018) 'Data protection: a tool kit for schools'
- The Data Protection Act 2018

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

- Acceptable Use Policy
- Allegations of Abuse Against Staff Policy
- Anti-Bullying Policy
- Behaviour Policy
- Complaints Procedure
- Data Protection Policy - GDPR
- E-Safety (including online safety) Policy
- Use of Mobile Phones and Digital Photography Policy

2. Roles and responsibilities

2.1. The Headteacher is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents 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 Procedures.

- 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 E-Safety Co-ordinator (currently the Headteacher) 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 and the school's Acceptable Use 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 to the Headteacher immediately.
- Attending any training on social media use offered by the school.

2.3. Parents are responsible for:

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

2.4. Pupils are responsible for:

- Adhering to the principles outlined in this policy and the school's E-Safety Rules (for KS1 or KS2 pupils as relevant).
- 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:

- School platforms such as *Google Classroom* or *Tapestry*
- 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, **"online bullying"** is defined as any use of social media or communication technology intentionally 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 parents when their children join the school using the Photograph Permission 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 duration of the pupil's time on roll at the school (unless later amended by the parents).

4.2. A record of consent is maintained (the Photo Permissions list), which details the nature of the consent for all pupils. The admin team are responsible for ensuring this consent record remains up-to-date. Class teachers will have access to this record, to enable the recording of images and videos in line with this policy, but will endeavour not to reveal to other children which pupils do not have image/video permission, since the school believes this personal decision to be a private one. The record should not, therefore, be displayed in the classroom, and efforts made to ensure pupils do not appear in images/videos should be discreet.

4.3. Parents are able to withdraw or amend their consent at any time. To do so, parents must inform the school in writing.

4.4. Consent can be requested for certain uses only: for example, consent for publication of images on the school website, but not on Twitter. This will be made explicitly clear on the consent from provided.

4.5. Where parents 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' and pupils' requirements following this.

4.6. 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 the school Twitter feed.

4.7. The school will only post images and videos of pupils for whom consent has been received.

4.8. Only school-owned devices will be used to take images and videos of the school community, with the exception of staff use of personal mobile phones to facilitate the rapid uploading of images/videos to the school's Twitter feed, as long as these media are then immediately removed from the personal device (ideally to storage on the school server).

4.9. When posting images and videos of pupils, the school may apply data minimisation techniques, such as pseudonymisation (blurring a photograph) to reduce the risk of a pupil being identified, if that is required or appropriate (e.g. if a whole-class photograph, which it is felt important to publish, would otherwise feature a pupil for whom consent has not been given for publication). However, school staff will ideally not record any videos or images featuring such pupils, or in the case of still images may arrange for the pupil to move to the periphery of a group prior to recording (enabling the ready cropping of the image before publication).

4.10. The school will not post pupils' personal details on social media platforms.

4.11. Pupils' 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 (e.g. it would not be suitable to display an image of a pupil in swimwear).

4.13. 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 (e.g. their name visible on a certificate or book that they are holding).

4.14. Any breaches of the data protection principles will be handled in accordance with the school's *Data Protection Policy – GDPR*.

4.15. Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos of school activities on personal accounts.

5. Social media use – staff

School accounts

5.1. School social media passwords are kept securely by the Headteacher – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the Headteacher.

5.2. Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements.

5.3. Staff will adhere to the data protection principles outlined in section 4 of this policy at all times.

5.4. Staff will not post any content online which is damaging to the school or any of its staff or pupils.

5.5. If inappropriate content is accessed online, a report form will be completed and passed on to the E-Safety Co-ordinator. The E-Safety Co-ordinator retains the right to monitor staff members' internet usage in line with the *Data Protection Policy – GDPR*

Personal accounts

5.6. Staff members will not access social media platforms during lesson times.

5.7. Staff members will not use any school-owned devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the Headteacher in such cases.

5.8. Staff members are permitted to use social media during break times.

5.9. Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the Headteacher, and once the E-Safety Co-ordinator has ensured any necessary network security controls are applied.

5.10. Staff will avoid using social media in front of pupils.

5.11. Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.

5.12. If pupils or parents attempt to "friend" a staff member, the staff member will report this to the Headteacher.

5.13. Staff members will not provide their home address, phone number, mobile phone number, social networking details or personal email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels (usually the class email address, not the individual staff member's school email account).

5.14. Staff members will ensure the necessary privacy controls are applied to personal accounts.

5.15. No staff member will post any content online that is damaging to the school or any of its staff or pupils.

5.16. Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of Huntington Community Primary School.

5.17. Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.

5.18. Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.

5.19. Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

5.20. 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 or disciplinary action (up to and including dismissal).

5.21. Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

5.22. 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.

5.23. Members of staff will not leave a computer or other device logged in when away from their desk, or save passwords such that devices can be logged into without manual password submission.

5.24. Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

6. Social media use – pupils and parents

6.1. Pupils will not access social media at school.

6.2. Pupils and parents will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts. Parents (not pupils) are only permitted to be affiliates of official school social media accounts (*Twitter* only at present).

6.3. Where a pupil or parent attempts to “friend” a staff member on their personal account, it will be reported to the Headteacher.

6.4. Pupils and parents will not post anonymously or under an alias to evade the guidance given in this policy.

6.5. Pupils and parents will not post any content online which is damaging to the school or any of its staff or pupils.

6.6. Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil’s age.

6.7. If inappropriate content is accessed online on school premises, it will be reported to the Headteacher.

6.8. Pupils are not permitted to use the school’s WiFi network to access any social media platforms.

6.9. Parents are not permitted to use the school’s WiFi network to access any social media platforms on personal devices.

6.10. 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. The school's network prevents access to certain websites through the use of *Smoothwall* filtering, provided by the school's ISP (Cheshire East). The following commonly-used social media websites are not accessible on the school's network:

- Facebook
- Instagram

7.2. Attempts made to circumvent the school network's security features 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 E-Safety Co-ordinator so that the site can be blocked.

7.4. The E-Safety Co-ordinator retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

7.5. Requests may be made to access erroneously blocked content by submitting a blocked content access form to the E-Safety Co-ordinator, which will be approved by the Headteacher (if not the same person).

8. Online bullying

8.1. Online bullying incidents are taken seriously at Huntington Community Primary School. Any reports of online bullying on social media platforms by pupils will be handled in accordance with the Anti-Bullying Policy.

8.2. Allegations of online bullying from staff members will be handled in accordance with the Allegations of Abuse against Staff Policy.

8.3. Staff members will not respond to or retaliate against online bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the Headteacher.

8.4. Evidence from any incident will be saved, including screenshots/photos of messages or web pages, and the time and date of the incident recorded.

8.5. Where the perpetrator is a current pupil or colleague, most incidents will 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 online bullying, regular education and discussion about E-Safety will take place as part of the Computing and PSHE curricula.

9. Training

9.1. At Huntington Community Primary School we recognise that early intervention can protect pupils who may be at risk of online bullying or negative social media behaviour. As such, teachers will receive training (where available) in identifying potentially at-risk pupils.

9.2. Teachers and support staff will receive training on the Social Media Policy as part of their induction.

9.3. Teachers and support staff will receive ongoing training in online safety as part of their development (through, for example, a subscription to SWGfL's *Boost* resources).

9.4. Pupils will be educated about E-Safety and appropriate social media use on an annual basis through a variety of means, including assemblies, PSHE lessons and activities organised by the E-Safety team.

9.5. Pupils will be provided with material to reinforce their knowledge, such as the online safety resources on the school website.

9.6. Parents will be invited to E-Safety and social media training on a regular basis and provided with relevant resources, such as the online safety resources on the school website.

9.7. 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 three–yearly basis by the Premises and Health & Safety Committee, in conjunction with the Headteacher, E-Safety Co-ordinator (if different) and DPO.

10.2. The next scheduled review date for this policy is Spring 2024.

10.3. Any changes made to this policy will be communicated to all staff, pupils and parents.

Blocked content access request form

Requester	
Staff name:	
Date:	
Full URL:	
Site content:	
Reasons for access:	
Identified risks and control measures:	
Authoriser	
Approved?	✓ / X
Reasons:	
Staff name:	
Date:	
Signature:	

Inappropriate content report form

Staff name (submitting report):	
Name of individual accessing inappropriate content (if known):	
Date:	
Full URL(s):	
Nature of inappropriate content:	
To be completed by E-Safety Co-ordinator	
Action taken:	
Staff name:	
Date:	
Signature:	