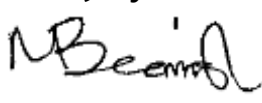




Bournville Primary School

Social Media Policy

Date Ratified: 15 July 2026

Signed By: 
On behalf of School Governors

Signed by :
Headteacher



Review Date: July 2027



Contents

Rationale	3
Scope	3
Organisational Control.....	4
Roles & Responsibilities	4
Process for creating new accounts.....	5
Monitoring	5
Behaviour.....	5
Legal Considerations.....	6
Legislation.....	6
Handling Abuse.....	7
Tone.....	7
Use of Images	7
Personal Use.....	8
Monitoring posts about the school.....	9
Appendix A - Managing your personal use of Social Media:	10
Appendix B - Managing school social media accounts	10



Social Media Policy

Rationale

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. However some games and video sharing platforms such as You Tube have social media elements to them.

Bournville Primary School recognises the numerous benefits and opportunities which a social media presence offers.

Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by Bournville Primary School, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements. This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

The school recognises that advances in artificial intelligence (AI) present new risks relating to the misuse, manipulation and redistribution of images of children. Before publishing any image or video online, staff must consider whether publication is necessary, proportionate and in the child's best interests. The existence of parental consent does not remove the requirement for a safeguarding risk assessment.



Organisational Control

Roles & Responsibilities

Senior Leadership Team (SLT)

- Facilitate training and disseminate guidance on Social Media use.
- Develop and implement the Social Media policy.
- Investigate any reported incidents whether internal or external.
- Make an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts.
- Approve account creation.
- Audit social media accounts for content and suitability

Administrator / Moderator

- Create social media accounts following SLT approval.
- Store account details, including passwords securely.
- Review and change passwords in line with acceptable use policy.
- Be involved in monitoring and contributing to the account.
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).
- Removing access to social media school accounts once a member of staff leaves
- Monitor and regulate online comments as posts are shared and remove when inappropriate.
- Where appropriate remove the facility for commenting on social media posts.
- Review social media presence in line with safer recruitment guidance prior to recruitment of candidates to ensure professional conduct or reputation cannot be questioned.

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
- Attend appropriate training.
- Regularly monitor, update and manage content they have posted via school accounts.
- Add an appropriate disclaimer to personal accounts when naming the school.
- Will not share passwords for school social media accounts.
- Review and change passwords in line with the acceptable use policy.
- Staff will only access school social media accounts on school devices
- Staff will understand and report new and emerging risks relating to online safety and social media. For example, those relating to:
 - AI-generated images and videos;
 - deepfake content;
 - online impersonation;
 - image-based abuse;
 - misinformation and disinformation;
 - cyberbullying;
 - online exploitation and grooming.



Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a “Friends of the school” Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt with standardised response. Negative or abusive comments will be met with a standardised response and an invitation to communicate directly with school. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- Any use of mobile phones and smart devices must comply with the school's Mobile Phone Policy and Acceptable Use Policy.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Staff should not respond to negative social media comments from followers or those engaging with the page. Instead they should defer comments to contact the school directly.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity
- If a member of staff is approached on social media by a pupil they should immediately report this to SLT and not accept any requests.
- If a journalist makes contact about posts made using social media staff must follow the school media policy and not respond. SLT must be contacted immediately should a journalist approach a member of staff on a social media platform.
- Unacceptable conduct, (e.g. sharing content that is considered to promote extremist views intended to radicalise, is defamatory,



discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal Considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Legislation

The following legislation must be considered when adhering to this policy:

- Obscene Publications Act 1959
- Protection of Children Act 1988
- Computer Misuse Act 1990, amended by the police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 2018
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- UK GDPR
- Data Protection Act 2018
- Online Safety Act 2023
- Keeping Children Safe in Education (current version)
- UKCIS guidance on sharing nude and semi-nude images
- DfE Mobile Phones in Schools guidance

Please note this list is intended to be indicative only.



Handling Abuse

- Those with social media access, will handle offensive comments swiftly and with a standardised response directing communication to SLT.
- If comments become offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Safe
- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of Images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Staff must not use personal mobile phones to photograph, film or record pupils.
- School-owned devices should be used wherever possible for educational photography and communication.
- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- The publication of photographs and videos of children must be subject to a safeguarding risk assessment. Consent alone does not remove safeguarding risks and professional judgement must always be exercised.
- Under no circumstances should staff share or upload pupil pictures online other than via school owned social media accounts.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- Images captured on authorised devices must be transferred promptly to secure school systems and removed from temporary storage locations.
- Staff must not view, save, forward, print or share nude or semi-nude images involving children.
- Any incident involving such imagery must be reported immediately to the DSL.
- Incidents will be managed in accordance with UKCIS and KCSIE guidance.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.



- Staff will not post a photograph that includes pupils/staff, when off site, in real time to advertise where they currently are. These should be scheduled to post when back in school environment or out of hours.

Personal Use

Staff

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Staff should follow the absence policy when reporting illness. It is inappropriate to use social media platforms to communicate absence from work. Such personal communications are within the scope of this policy

Colleagues at school are advised not to write about their work but where a colleague chooses to do so:

- Staff should make it clear that the views expressed are theirs only and do not reflect the views of the school/Trust. They must not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act or disclose any information about the school/Trust that is not yet in the public arena
- Colleagues at the school should not post photographs of pupils under any circumstances and should not post photographs of colleagues or parents without their express permission
- Colleagues at the school should not disclose confidential information relating to their employment at the school
- No colleague at the school should use any internet/online resources to seek information on any pupil, parent or other colleague at the school other than for the purposes of legitimate monitoring of the usage of social networking sites by designated managers/officers
- Colleagues at the school should not use social networking sites to seek to influence pupils regarding their own political or religious views or recruit them to an organisation of this kind using their status as a trusted adult to encourage this
- Report to the SLT, school designated safeguarding teacher/officer or line manager any occasions when a pupil attempts to involve them in on-line or social networking activity
- Colleagues at the school should not share any personal information with any pupil (including personal contact details, personal website addresses/social networking site details)
- Colleagues at the school should not place/post any material (or links to any material) of a compromising nature (that is any material a reasonable person might find obscene or offensive (such as sexually explicit or unlawfully discriminatory material) including inappropriate photographs or indecent remarks or material relating to illegal activity) on any social network space.
- Colleagues at the school are strongly advised, in their own interests, to take steps to ensure that their on-line personal data is not accessible to anybody who they do not want to have permission to access it. For example, they are advised to check security and privacy settings of any social networking site they subscribe to and set these to a maximum



- The school reserves the right to take action to obtain the removal of any content posted by colleagues at the school which may adversely affect the reputation of the school (or any colleague, governor, pupil or parent at the school) or put it at risk of legal action. Should the school decide to pursue this course of action, the advice of the ELAN Central Team may be sought.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken, following the acceptable use policy.
- The school permits reasonable and appropriate access to private social media sites.

Pupils

- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account. Staff must inform the Designated Safeguarding Lead should a request be made for action.
- The school's education programme should enable pupils to be safe and responsible users of social media
- Pupils are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- The school will use the approved monitoring systems identified by the Online Safety Lead and Trust to monitor whenever the school is mentioned on the Internet. The Online Safety Leader will receive alerts and monitor regularly.
- Where an online media comment is not appropriate a standard comment will be generated such as; 'Thank you for your comment, please phone the school to discuss your concerns – 01934 427130'



Appendix A - Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don’t use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to offer challenge, do it politely and respectfully
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Appendix B - Managing school social media accounts

The Do’s

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure commenting is turned off
- Ensure you have permission to ‘share’ other peoples’ materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school’s reporting process
- Consider turning off tagging people in images where possible.

The Don’ts

- Don’t make comments, post content or link to materials that will bring the school into disrepute
- Don’t publish confidential or commercially sensitive material
- Don’t breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don’t link to, embed or add potentially inappropriate content
- Don’t post derogatory, defamatory, offensive, harassing or discriminatory content
- Don’t use social media to air internal grievances.