Bushfield Road Infant School

Social Media Policy

Date approved: November 2026
Review date: November 2028

1. Purpose

Bushfield Road Infant School uses social media to communicate with families and the wider community, celebrate pupils' learning and achievements, and share school news.

All activity must protect pupils, families and staff, and reflect the school's values of **Kindness, Teamwork and Curiosity**.

2. Scope

This policy applies to staff, governors, volunteers, contractors and any other person authorised to post on behalf of the school.

It covers official school social media accounts, including Facebook and Instagram, and any other platform the school chooses to use. It should be read alongside the school's safeguarding and child protection policy, staff code of conduct, data protection and privacy information, and complaints procedure.

3. Who may post

- Only the Headteacher, Deputy Headteacher may publish content or respond on official accounts.
- Access must be limited to trained to the Head and Deputy. At least two authorised staff should be able to manage the accounts so they can be monitored during absence.
- Staff must not use personal social media accounts to post on behalf of the school or use personal messaging accounts to communicate with pupils or families about school matters.

- Staff must not share school content from an official account through a personal account unless authorised to do so.

4. Publishing content and images

Before publishing, authorised staff must check that:

- the information is accurate, appropriate and approved for public sharing;
- the content does not reveal confidential information or put a pupil, family member or member of staff at risk;
- any pupil who could be identified in an image or video is cleared for that specific type of use under the school's current image-permission records and data protection arrangements;
- any safeguarding or other restriction has been checked with the Designated Safeguarding Lead (DSL) or Deputy DSL where necessary.

The school will explain to families how pupil images may be used and where they may appear. The school's DPO will advise on the lawful basis for using images and how permissions, objections or withdrawal requests are recorded. Staff must not assume that a general permission covers every platform or purpose.

Use school equipment to take and store images. Staff must not use personal devices unless specifically authorised under school procedures. Images must be transferred and stored securely, and deleted in line with the school's retention arrangements.

Do not publish a pupil's full name alongside their image, or include other identifying details, unless this has been specifically approved and is covered by the school's arrangements. Never publish information that could identify a pupil whose safety or welfare may be compromised.

5. What the school may post

Appropriate content may include:

- school events, trips and activities;
- examples of learning and pupil work, where these do not reveal personal information;
- school news, reminders and information for families;
- achievements and positive contributions by pupils and the school community.

Posts should be respectful, inclusive and consistent with the school's values. Avoid posting details that reveal a pupil's routine, live location, personal circumstances or other information that could create a safeguarding or privacy risk.

6. Comments, messages and online concerns

Authorised staff must check comments and messages regularly during the school working week.

- Remove or hide comments that contain personal information, abusive or discriminatory language, threats, spam, or content that is inappropriate for a school account.
- Do not argue publicly, disclose confidential information, or discuss an individual pupil, family or member of staff online.
- Refer complaints or concerns to the appropriate school process; do not investigate or resolve individual cases through social media.
- Pass any safeguarding concern, threat or disclosure to the DSL or Deputy DSL **without delay** and follow the school's safeguarding procedures.
- Record relevant decisions and actions in the appropriate school system. Social media messages must not replace the school's formal safeguarding records.

The DSL is **Mr Vessey**. The Headteacher must ensure the policy and account information show the current DSL and Deputy DSL.

7. Account security

- Use strong, unique passwords and multi-factor authentication where available.
- Store passwords securely; do not share them through group messages or with unauthorised people.
- Review account access when an authorised member of staff changes role or leaves.
- Report suspected loss of access, hacking, impersonation or accidental disclosure immediately to the Headteacher and the school's IT or data protection lead. Follow the school's data-breach and safeguarding procedures where relevant.

8. Staff use of personal social media

Staff must maintain professional boundaries online and follow the school's code of conduct. They must not identify pupils or families, disclose confidential school information, or communicate privately with pupils through personal accounts. Concerns about online conduct, including content that targets or harasses staff, should be reported through the school's established procedures.

9. Responsibilities and review

The Headteacher oversees this policy and the school's official accounts. Authorised staff are responsible for following the policy when preparing or publishing content. The DSL advises on safeguarding risks; the DPO advises on data protection and image-use arrangements.

The school will review the policy at least every two years and after any significant change to its social media use, or following a relevant incident. Any suspected safeguarding issue must be handled through the school's safeguarding procedures, not left until the policy review.

Sources

- *Keeping children safe in education 2026*, Department for Education. (gov.uk)
- *Data protection in schools: Taking and using photos and videos*, Department for Education. (gov.uk)
- *Taking photographs: data protection advice for schools*, Information Commissioner's Office. (ico.org.uk)
- *Online safety guidance for staff*, Department for Education. (gov.uk)