

Social Media Policy

The British School

Working together for our children's future



Approved by:	Abel Roche	Date: April 2026
Last reviewed on:	September 2025	
Next review due by:	April 2027	

1. Purpose and Safeguarding Context

The purpose of this policy is to ensure safe, responsible and appropriate use of social media in order to:

- Set guidelines and rules on the use of social media channels
- Set clear expectations for the way members of the school community engage with each other online.
- Support the school's policies on data protection, online safety and safeguarding.
- Protect children from online harm.
- Maintain professional boundaries.
- Safeguard personal data.
- Protect the reputation of the school.

In line with *Keeping Children Safe in Education*, online safety is treated as an integral part of the school's overall safeguarding approach and is reflected consistently across related policies.

This policy applies to **staff, pupils, parents/carers, governors and volunteers**, and covers both **professional and personal use** of social media, regardless of time, location or device.

2. Definition of Social Media

Social media refers to any online platform or digital service that enables users to communicate, share content (including videos and photos) or interact with others. This includes (but is not limited to):

- Social networking platforms.
- Messaging apps and group chats (e.g. WhatsApp).
- Photo and video-sharing services.
- Blogs, forums and gaming communication tools.

3. Official School Social Media Accounts

The school currently operates official accounts on:

- Facebook.
- Instagram.

Governance and Oversight

- All official accounts are controlled and monitored by the **Headteacher**.
- Access is restricted to authorised staff only.
- Content is reviewed to ensure accuracy, appropriateness and safeguarding compliance.

Permitted Content

- School news and announcements.
- Alerts about changes (e.g. procedures, severe weather updates) reminders
- Educational activities and events.
- Celebrations and achievements.
- Recruitment information.
- Photographs of pupils **where written consent has been obtained**.

Prohibited Content

- Content that is discriminatory, inflammatory, unsafe, harmful or abusive.

- Identifiable personal data of pupils or staff.
- Images without consent.
- Political messaging.
- Commercial advertising.
- Content that is discriminatory, inflammatory or unsafe.

Moderation

Comments and content may be removed if they are abusive, defamatory, discriminatory or breach data protection. Persistent misuse may result in restricted access. Formal complaints must follow the school complaints procedure.

4. Staff Use of Social Media

In line with DfE and Ofsted expectations regarding professional conduct and safeguarding boundaries, staff must:

Staff Must Not:

- Use personal social media accounts for school business.
- Communicate with pupils (current or former) via personal accounts.
- Accept friend or follow requests from pupils.
- Post images of pupils.
- Discuss school matters, pupils, parents or colleagues online.
- Represent personal views as those of the school.
- Link personal social media accounts to school contact details.

Any social media contact initiated by a pupil must be reported immediately to the **Designated Safeguarding Lead (DSL)**.

Concerns will be addressed under the **Staff Behaviour Policy** and safeguarding procedures.

5. Pupils' Use of Social Media

Pupils are taught about online safety through a planned and progressive curriculum, in line with DfE statutory guidance.

Pupils are expected to:

- Communicate respectfully online.
- Avoid sharing harmful or inappropriate content.
- Understand how to report concerns.

Incidents involving misuse of social media will be managed under the **Behaviour Policy** and safeguarding procedures where appropriate.

6. Parents and Carers

Parents and carers are expected to:

- Model respectful online behaviour.
- Raise concerns through appropriate school channels.
- Not post content that could harm individuals or the school's reputation.

WhatsApp and Informal Groups

Expectations within this policy apply equally to parent-led messaging groups. The school does not monitor these groups and will not respond to concerns raised via social media.

7. Images, Consent and Data Protection

In line with GDPR and safeguarding guidance:

- Written parental consent is required before images are taken or shared.
- Consent is reviewed annually.
- Images are stored securely.
- Personal devices must not be used to photograph pupils.

All image use follows NSPCC and DfE safeguarding guidance.

8. Training, Monitoring and Review

- Online safety training forms part of staff safeguarding training and induction.
- Pupils are taught online safety regularly, not as a one-off event.
- Leaders monitor the effectiveness of this policy as part of safeguarding oversight.

The policy is reviewed **annually** to reflect changes in legislation, guidance and online risk.

9. Related Policies

- Safeguarding and Child Protection Policy.
- Behaviour Policy.
- Staff Behaviour Policy.
- ICT and Acceptable Use Policy.
- Mobile Phone Policy.
- Photography and Filming Policy.

Appendix A: Safeguarding Use of Images and Photography (NSPCC-Aligned)

A1. Purpose and Scope

This appendix sets out clear procedures for the safe taking, use, storage and sharing of images and videos of children, in line with NSPCC guidance, GDPR and *Keeping Children Safe in Education*.

It applies to **all staff, volunteers, visitors, contractors and external professionals**.

The aims are to:

- Protect children from harm or misuse of images.
- Ensure lawful, ethical and proportionate use of photography.
- Provide clarity for staff, pupils and families.

A2. Safeguarding Principles

The school's approach is based on the following principles:

- The welfare of children is paramount.
- Children should never experience abuse of any kind.
- Families have the right to informed choice.
- Images must only be used for legitimate school purposes.
- Online publication carries additional risk.

A3. Consent and Lawful Use

- Written parental consent is required before images are taken or shared.
- Where appropriate, children's views will also be considered.
- Consent explains **purpose, audience, storage and duration**.
- Families are informed that once published, complete removal may not always be possible.
- Consent is required annually.

A4. Taking and Using Images Safely

To minimise risk, the school will:

- Avoid publishing identifiable personal information.
- Use first names only where identification is necessary.
- Ensure children are appropriately dressed.
- Avoid imagery that increases the risk of misuse.
- Use images that positively reflect children's participation.

A5. Personal Photography at School Events

Where parents, carers or spectators take images for personal use:

- Clear guidance will be communicated before or at events.
- Sharing images on social media without consent is discouraged.
- Concerns about image use can be raised with school leaders.

The school does not police personal devices but will act where safeguarding concerns arise.

A6. Photography for School Purposes

- School photography must be authorised by senior leaders.
- Only school-owned equipment may be used.
- Personal devices must not be used at any time.
- Photography for curricular purposes must be proportionate and planned.

Professional photographers:

- Receive a clear safeguarding brief.
- Must be identifiable at all times.
- Are supervised and not given unsupervised access to children.
- Must not conduct off-site or private sessions.
- Any concerns are reported through safeguarding procedures.

A7. External or Media Photography

External photographers (e.g. press or media) must seek permission in advance and provide:

- Purpose and intended use of images.
- Details of the photographer.

Consent will be confirmed before images are taken. Anyone acting outside permission will be asked to leave and safeguarding procedures followed if necessary.

A8. Storage, Security and Retention

Images will be:

- Stored securely in line with GDPR.
- Held on protected systems with restricted access.
- Never stored on personal or unencrypted devices.
- Retained only for as long as necessary.

A9. Refusal or Withdrawal of Consent

Where consent is not given or is withdrawn:

- The child's wishes are respected.
- Arrangements are made discreetly.
- No child is excluded or disadvantaged.

A10. Related Policies

- Safeguarding and Child Protection Policy.
- Staff Code of Conduct.
- Online Safety Policy.
- Data Protection Policy.