



Pensans Community Primary School

Social Media Policy

Approved by	Trust Board
Review date	September 2026
Next review date	September 2027
Policy owner	Headteacher

1. Introduction

Social media can be a valuable way for Pensans Community Primary School to celebrate pupils' achievements, communicate with families, promote school life and build positive relationships with the wider community. It also creates risks involving safeguarding, privacy, data protection, cyber security, professional boundaries, misinformation and online abuse.

This policy sets clear expectations for the use of the school's official social media accounts and for staff, volunteers and contractors when using personal social media in a way that could affect their professional role or the school community.

Everyone using social media in connection with the school must act professionally, protect children and colleagues, respect confidentiality and follow the school's safeguarding, behaviour, acceptable-use, data-protection and staff code-of-conduct requirements.

2. Policy Scope and Responsibilities

This policy applies to all employees, supply staff, volunteers, contractors and other adults working for or on behalf of the school. It applies whether social media is accessed on school premises, while working remotely, during school activities or outside normal working hours where the activity has a professional connection or could reasonably affect the school, pupils, families or colleagues.

The Headteacher has overall responsibility for ensuring that the school's social media activity is safe, appropriate and consistent with school and Trust expectations.

Only authorised staff may publish through official school social media accounts. Access should be limited to trained staff and should not depend on a single individual. At least two appropriate authorised adults should have suitable access arrangements so that the school is not dependent on one person during absence.

All staff are responsible for their own online conduct and for raising concerns promptly with the Headteacher or Designated Safeguarding Lead (DSL), as appropriate.

3. School Social Media Content

Official school accounts may be used for appropriate school-related content such as events and announcements, celebrations and achievements, curriculum and learning, community information, school news, recruitment and approved photographs or videos.

Content must be accurate, proportionate, inclusive and suitable for a public audience. Posts should be positive and professional and should reflect the school's values.

Staff must not publish content simply because it is available to them. Before posting, consider whether the post is necessary, accurate, respectful, safe and appropriate for a primary-school audience.

If unsure, do not post. Seek advice from the Headteacher or another authorised senior member of staff.

4. Safeguarding, Pupils and Professional Boundaries

Safeguarding is everyone's responsibility. Online activity must never compromise a child's safety, dignity or privacy.

Staff must not accept or initiate personal social-media connections with current pupils. Staff should also avoid personal social-media connections with former pupils where this could create a professional-boundary concern. School communication with pupils and families must use approved school systems.

Staff must not communicate privately with pupils through personal social-media accounts, direct messages, personal email accounts or personal messaging services. Any safeguarding concern arising from online contact must be reported to the DSL without delay.

Staff must not share information that could identify a child unnecessarily, including full names alongside photographs, addresses, personal contact details, medical information, safeguarding information, attendance information or other sensitive information.

Where online material raises a safeguarding concern, preserve relevant evidence and report it through the school's safeguarding procedures. Do not investigate beyond your role or engage in online confrontation.

5. Photographs, Video and Personal Data

Photographs and videos of pupils are personal data where individuals can be identified. The school must use an appropriate lawful basis and follow its data-protection arrangements when taking, storing or publishing images.

Before publication, staff must check the school's current permissions/opt-out records and ensure that the proposed use is covered. Social media is a public or potentially wide-reaching environment and therefore requires particular care.

Images must be appropriate, respectful and representative of school life. Avoid unnecessary identifying information, including pupil full names, locations, routines or other details that could increase risk.

School devices or other school-approved equipment should be used for official photography. Personal devices must not be used to take or store pupil images unless this is expressly permitted by the school's procedures.

Images and videos must be stored securely, shared only with appropriate people and deleted or retained in accordance with the school's data-retention arrangements.

Parents and carers should be given clear information about how images may be used and should be directed to the school's privacy information where appropriate.

6. Personal Social Media Use by Staff

Staff have a right to a private life and may use social media personally. However, staff must maintain appropriate professional boundaries and must not post material that breaches confidentiality, safeguarding requirements, employment duties or the school's staff code of conduct.

Do not identify pupils, families or colleagues in connection with confidential or sensitive matters. Do not post screenshots, messages, photographs or other material obtained through school systems unless authorised.

Do not use personal social-media accounts to conduct school business. Use the school's approved email, communication and information-sharing systems.

Staff should review privacy and security settings regularly, use strong unique passwords and multi-factor authentication where available, and be alert to phishing, impersonation and social-engineering attempts.

Staff should not assume that content is private because an account is restricted. Posts may be copied, shared or screenshotted.

7. Prohibited and High-Risk Activity

Users must not use social media to harass, threaten, bully, discriminate against or intimidate others; share unlawful, abusive, hateful or sexually inappropriate material; disclose confidential school information; impersonate the school or another person; or make statements on behalf of the school without authority.

Do not post content that could reasonably bring the school or Trust into disrepute, undermine professional relationships, compromise safeguarding or damage trust with pupils, parents, carers or colleagues.

Do not publish political, religious or personal campaigning content through official school accounts. Official accounts must remain focused on the school and its community.

Do not use social media to respond to complaints, allegations or contentious incidents in a way that escalates the situation. Refer complaints through the school's complaints procedure and refer safeguarding concerns to the DSL.

8. Managing Comments, Complaints and Online Abuse

Official accounts should be monitored by authorised staff. Comments or messages that are abusive, discriminatory, threatening, defamatory, disclose personal information or otherwise breach the platform's rules may be hidden, removed or reported where appropriate.

The school should not argue with members of the public online. A calm, factual and proportionate response should be used where a response is appropriate.

Complaints about the school should normally be directed to the school's complaints procedure. Staff should not attempt to resolve formal complaints through personal social-media accounts.

If a member of staff experiences online bullying or harassment, they should not retaliate. Save evidence such as screenshots, URLs and dates, and report the matter to a senior leader. The school will consider appropriate support and action.

Threats, serious harassment, hate crime or other potentially criminal activity should be considered for referral to the police or other appropriate agencies.

9. Cyber Security and Account Management

Official social-media accounts must be protected using strong passwords, secure recovery arrangements and multi-factor authentication where available.

Passwords must not be shared through insecure channels or stored in an openly accessible document. Access should be removed promptly when a member of staff changes role or leaves the school.

New social-media accounts, apps, scheduling tools or third-party services must not be connected to school accounts without appropriate approval.

Staff must remain alert to phishing, fake competitions, malicious links, impersonation accounts and requests for passwords or verification codes. Suspicious activity must be reported immediately.

Where an account is compromised, staff must stop posting, preserve evidence and inform the Headteacher or appropriate senior leader so that access can be secured and the incident managed.

10. Crisis and Sensitive Incidents

During safeguarding incidents, serious complaints, critical incidents, accidents, police matters, cyber incidents or other sensitive situations, staff must not post about the incident unless expressly authorised.

Only the Headteacher or an authorised person should issue official statements on behalf of the school. Staff must not speculate, confirm rumours or comment on investigations.

Where information must be communicated urgently, the school will use its approved communication systems and follow relevant emergency, safeguarding and business-continuity procedures.

11. Policy Enforcement

Failure to follow this policy may be treated as a disciplinary matter. Depending on the circumstances, breaches may also lead to safeguarding action, referral to the police, data-protection investigation, removal of access or other appropriate action.

Nothing in this policy prevents staff from raising genuine safeguarding, whistleblowing, equality or other protected concerns through appropriate channels.

The school will support staff who experience online abuse or harassment and will take proportionate action in line with current Department for Education guidance and the school's employment procedures.

12. Related Policies and Guidance

Staff should read this policy alongside the school's Online Safety Policy, Acceptable Use Policy, Child Protection and Safeguarding Policy, Staff Code of Conduct/Behaviour Policy, Data Protection and Privacy arrangements, Complaints Policy and relevant emergency procedures.

Current external guidance informing this policy includes Keeping Children Safe in Education 2026; Department for Education guidance on online safety and bullying/harassment of school staff; Department for Education data-protection guidance for schools; and Information Commissioner's Office guidance on children's information and photographs.

13. Staff Acknowledgement

I confirm that I have read and understood the Pensans Community Primary School Social Media Policy and understand my responsibilities when using official school social-media accounts and personal social media.

[illegible]

Policy note: This acknowledgement records that staff have received and understood the policy. It does not replace the school's safeguarding, data-protection or staff conduct procedures.