Wittersham Church of England Social Media Policy 2026

We strive to cooperate and work alongside all members of our community to feel valued, nurtured, and empowered as they embark upon their journey to become the very best that God intended. Throughout their voyage of discovery with us, we ensure all children are provided with a rich curriculum, and experiences that promote courage and a strong moral purpose underpinned by our Christian values; preparing them to become compassionate citizens within our rural community and the wider world.

Revision History

Version	Date	By	Description
V03	February 2025	Stella Coulson	Annual Review
V04	September 2026	Stella Coulson	Updated policy reference to the Children's Wellbeing and Schools Act 2026.

1. Policy Statement

Wittersham Church of England Primary School recognises that social media and online communication form an important part of modern life.

When used appropriately, social media can provide valuable opportunities for communication, celebration, learning and community engagement. However, inappropriate or unsafe use can expose children and adults to safeguarding, privacy, reputational and well-being risks.

The school is committed to promoting safe, responsible, respectful and age-appropriate use of social media and online communication.

Safeguarding children remains paramount in all decisions relating to social media.

The same standards of behaviour, respect and professionalism expected offline apply online.

2. Aims

This policy aims to:

- safeguard and promote the welfare of children when using or being affected by social media;
- establish clear expectations for pupils, staff, governors, volunteers, parents/carers and others associated with the school;
- maintain appropriate professional boundaries between staff and pupils/families;
- protect children and adults from online abuse, harassment, bullying and exploitation;
- protect personal information, photographs and other data;
- promote responsible digital citizenship;
- support children's understanding of online risks;
- protect the professional reputation of staff and the school;
- establish appropriate arrangements for official school social-media accounts; and
- ensure concerns arising through social media are identified, reported and responded to appropriately.

3. Legislation and Statutory Guidance

This policy has regard to:

- Keeping Children Safe in Education 2026;

- the Children's Wellbeing and Schools Act 2026;
- Working Together to Safeguard Children;
- the Online Safety Act 2023;
- the Education Act 1996;
- the Equality Act 2010;
- the Data Protection Act 2018 and UK GDPR;
- the Prevent duty;
- the statutory EYFS framework 2026 where applicable;
- relevant DfE guidance on mobile phones and personal devices in schools; and
- Kent Safeguarding Children Multi-Agency Partnership procedures.

KCSIE 2026 is now in force and requires all school staff to read Part One in full and follow their school's safeguarding policies and procedures. It specifically recognises online harms as part of safeguarding.

The Children's Wellbeing and Schools Act 2026 also introduces provisions relating to children's online well-being and requires schools to have regard to government guidance concerning pupils' use and access to mobile phones and other personal interactive communication devices during school hours.

4. Scope

This policy applies to:

- pupils;
- parents and carers;
- teaching staff;
- support staff;
- the Headteacher and senior leaders;
- governors;
- volunteers;
- contractors;
- students;
- visitors; and
- anyone providing services on behalf of the school.

It applies to the use of social media both on and off school premises where that use has a connection with the school, a child, a member of staff or the wider school community.

5. Definition of Social Media and Online Communication

For the purposes of this policy, social media includes any online service enabling users to communicate, interact, create or share content.

This includes, but is not limited to:

- social networking platforms;
- video and image-sharing platforms;
- messaging applications;
- group chats;
- online forums;
- gaming platforms with communication functions;
- livestreaming services;
- blogs;
- discussion boards;
- community groups;
- collaborative online spaces;
- AI-enabled social or communication services; and
- any emerging platform offering similar functionality.

The policy applies regardless of whether an account is public, private, anonymous, temporary or restricted.

6. Safeguarding and Online Safety

Online safety is an integral part of safeguarding.

The DSL has overall responsibility for safeguarding and online safety within the school.

Staff must recognise that safeguarding concerns can arise through:

- social media;
- messaging applications;
- online games;
- livestreaming;
- image and video sharing;
- group chats;
- AI-enabled services;
- inappropriate contact;
- online bullying;
- sexual harassment;

- grooming;
- exploitation;
- coercion;
- harmful content;
- misinformation and disinformation; and
- the sharing of personal information.

Staff must act immediately on safeguarding concerns and report them to the DSL or a Deputy DSL without delay. KCSIE 2026 reinforces that safeguarding concerns must be acted upon immediately and appropriately recorded.

7. General Expectations

All members of the Wittersham community are expected to communicate online positively and responsibly.

Online communication should reflect our school values of Compassion, Courage and Cooperation.

Members of the school community should not post, share, create or endorse content which:

- threatens or intimidates another person;
- constitutes bullying or harassment;
- is discriminatory;
- is defamatory;
- compromises safeguarding;
- breaches confidentiality;
- contains personal information without appropriate authority;
- deliberately damages the reputation of an individual or the school; or
- is otherwise unlawful or inappropriate.

8. Staff Use of Social Media

Staff are entitled to use social media in their personal lives.

However, staff must recognise that their online behaviour can affect:

- their professional reputation;
- public confidence in them;
- their relationship with pupils and families;
- colleagues;
- safeguarding; and

- the reputation of the school.

Staff must maintain appropriate professional standards online regardless of whether an account is described as private or personal.

Privacy settings do not remove an individual's professional responsibilities.

9. Personal Social-Media Accounts

Staff should maintain appropriate privacy settings on personal accounts and regularly review these.

Staff should:

- use strong and secure passwords;
- use multi-factor authentication where available;
- consider carefully what personal information is publicly accessible;
- disable unnecessary location sharing;
- consider whether posts could reasonably be associated with their professional role;
- avoid representing personal views as those of Wittersham;
- consider the permanence and shareability of online content; and
- report concerns where personal online activity may affect their professional role.

10. Staff Contact with Pupils

Staff must not use personal social-media accounts to communicate privately with current pupils.

Staff must not:

- add or accept current pupils as friends, followers or contacts through personal accounts;
- privately message pupils using personal accounts;
- communicate with pupils through disappearing-message functions;
- establish unofficial pupil group chats;
- share personal contact information for social-media communication; or
- move school-related conversations onto personal social-media accounts.

Any unsolicited contact from a pupil through a personal account should not normally be responded to and must be reported where there is a safeguarding or professional-boundary concern.

Official school-approved communication channels must be used.

11. Staff Contact with Parents and Carers

Staff should not ordinarily use personal social-media accounts to communicate with parents/carers about school matters.

Staff should not routinely add or accept current pupils' parents/carers as friends or contacts on personal accounts.

The school recognises that Wittersham is a small rural community and that genuine pre-existing relationships may exist.

Where a pre-existing relationship means this expectation cannot reasonably be followed, the member of staff should discuss the circumstances with the Headteacher/DSL.

Appropriate professional boundaries must continue to be maintained.

12. Former Pupils

Staff should exercise particular caution regarding social-media contact with former pupils.

The fact that a child has left Wittersham does not automatically remove safeguarding or professional-boundary considerations.

Where ongoing contact is required for a legitimate educational purpose, official school-approved communication methods should be used.

13. Confidentiality

Staff must never disclose through social media:

- confidential pupil information;
- safeguarding information;
- SEND or medical information;
- personal information about pupils or families;
- confidential staff information;
- internal school matters not intended for publication; or
- photographs, videos or other material for which appropriate permission has not been obtained.

Information accessed through employment remains confidential regardless of whether the member of staff is using a personal device or account.

14. Photographs and Videos

Photographs or videos of pupils may only be published through official school channels in accordance with:

- parental consent;
- the school's image-use arrangements;
- safeguarding requirements; and
- data-protection requirements.

Staff must not publish photographs or videos of pupils on their personal social-media accounts.

Care must be taken that images do not inadvertently disclose sensitive information, including a child's location, personal circumstances or other identifying information.

15. Official School Social Media

Official school social-media accounts may only be established or operated with the approval of the Headteacher.

Official accounts must:

- have a clear educational, communication or community purpose;
- use school-controlled contact details;
- be appropriately secured;
- have more than one authorised member of staff able to access the account where practicable;
- use appropriate privacy and security settings;
- comply with safeguarding and data-protection requirements;
- use images only where appropriate consent exists;
- maintain professional language and tone; and
- be capable of appropriate leadership oversight.

16. Direct Messaging Through Official Accounts

Official school social-media accounts should not ordinarily be used for private one-to-one conversations with pupils.

Where parents contact the school through direct messaging, staff should consider whether the conversation should be moved to an official school communication system or email.

Safeguarding information received through social media must be reported and recorded through the school's safeguarding procedures.

17. Staff Managing Official Accounts

Staff operating an official account must:

- be authorised by the Headteacher;
- understand the Acceptable Use Policy;
- act as a representative of Wittersham;
- communicate professionally;
- comply with safeguarding, equality, confidentiality, copyright and data-protection requirements;
- not make commitments on behalf of the school without authority;
- not engage in inappropriate debate or argument online; and
- report concerning contact or content promptly.

18. Pupils' Use of Social Media

Personal use of social media by pupils during the school day is not permitted.

The school recognises that many social-media services impose minimum age requirements and that primary-aged pupils may not meet those requirements.

The school will not create pupil accounts on services where children do not meet the platform's applicable minimum-age requirements.

Pupils will be taught not to misrepresent their age in order to access age-restricted platforms.

19. Children's Wellbeing and Schools Act 2026 – Personal Devices

Wittersham is committed to providing a school environment in which children can learn, play, communicate and develop relationships without unnecessary distraction from personal digital devices.

The Children's Wellbeing and Schools Act 2026 requires schools in England to have regard to government guidance concerning pupils having and using mobile phones and other personal interactive communication devices during school hours.

Wittersham's arrangements for pupils' personal devices are set out in the school's relevant Mobile Phone/Personal Device and Behaviour procedures.

Where a pupil is permitted to bring a device to school for a specific agreed reason, the school's arrangements for storage, access and use must be followed.

Exceptions may be agreed where necessary for medical, SEND, safeguarding or other individual needs.

20. Underage Social-Media Use

The school recognises that some primary-aged children may access social-media platforms outside school, including platforms for which they do not meet the stated minimum age requirement. Many widely used social-media platforms set a minimum account age of 13, although age requirements vary between services. The school does not encourage pupils to create or use accounts where they do not meet the platform's age requirements.

The school will take a safeguarding and educational approach to underage social-media use. Pupils will be taught, in an age-appropriate way, about online safety, privacy, responsible communication, harmful or inappropriate content, online relationships, reporting concerns and how to seek help if something online makes them feel worried, uncomfortable or unsafe.

Where the school becomes aware that a pupil is using a social-media platform for which they do not meet the minimum age requirement, staff will consider:

- the child's age and level of understanding;
- the platform involved and its stated age requirements;
- the nature and frequency of the child's use;
- whether the child is communicating with known or unknown individuals;
- the type of content being viewed, created or shared;
- whether personal information, images or location information have been shared;
- parental or carer awareness and supervision;
- whether there are concerns relating to bullying, harassment, exploitation, grooming, inappropriate contact or harmful content;
- whether the use is affecting the child's wellbeing, behaviour, relationships, attendance or learning;
- whether there is a safeguarding concern requiring further action; and
- whether additional education, pastoral support or intervention is required.

Parents/carers will normally be informed where appropriate and will be encouraged to support safe, age-appropriate use of technology at home.

Where social-media use gives rise to a safeguarding concern, staff must follow the school's Child Protection and Safeguarding Policy and report the concern promptly through the school's safeguarding procedures. Where necessary, the school may seek advice from or make referrals to appropriate external agencies.

The school will not rely solely on age restrictions when responding to concerns. Its primary consideration will be the safety, welfare and best interests of the child.

21. Social Media and Children's Online Well-being

The school recognises the potential impact of online environments on children's emotional well-being, sleep, self-esteem, relationships, concentration, behaviour, body image, understanding of the world and exposure to inappropriate or harmful material.

The Children's Wellbeing and Schools Act 2026 provides powers for the Government to introduce regulations requiring providers of internet services to prevent or restrict children's access to particular services, features or functions where this is necessary to protect children from harm.

The Government has announced that social-media companies will be prevented from offering certain social-media services to children under the age of 16. The Government intends to lay the first regulations before Parliament by the end of 2026, with the restrictions expected to come into force in spring 2027.

Until those regulations come into force, the school will continue to follow current statutory requirements, safeguarding guidance and individual platforms' applicable age requirements.

The school will keep its approach to social media and online safety under review as regulations and statutory guidance are introduced or updated.

22. Online Safety Education

Wittersham will provide age-appropriate online-safety education throughout the curriculum.

Children will learn about:

- privacy;
- personal information;
- safe passwords;
- age restrictions;

- respectful communication;
- online friendships;
- cyberbullying;
- harmful content;
- inappropriate contact;
- grooming and exploitation;
- image sharing;
- scams;
- misinformation and disinformation;
- reporting and blocking;
- seeking help from a trusted adult;
- the permanence of online content;
- algorithms and personalised content where age appropriate; and
- safe and responsible use of artificial intelligence.

Government plans for RSHE from September 2026 include increased critical thinking about AI and AI chatbots, misinformation and disinformation, and misogynistic or violent online content.

23. Artificial Intelligence and Emerging Technology

The school recognises that social-media platforms increasingly incorporate artificial intelligence, recommendation systems, chatbots, image-generation tools and other emerging technologies.

Children will be taught, at an age-appropriate level, that:

- AI-generated information may be inaccurate;
- AI-generated images, video and audio may appear genuine when they are not;
- personal information should not be entered into inappropriate AI services;
- AI chatbots are not substitutes for trusted adults;
- generated content can still cause harm;
- technology can reinforce bias or misinformation; and
- concerning AI-generated material should be shown to a trusted adult.

Staff must use school-approved technology in accordance with school policies and safeguarding, confidentiality and data-protection requirements.

24. Cyberbullying and Online Harassment

Online bullying, harassment or intimidation involving members of the school community will

be taken seriously.

This includes behaviour occurring outside school where it:

- affects a child's welfare;
- affects relationships within school;
- creates a safeguarding concern;
- impacts staff safety or welfare; or
- significantly affects the orderly operation of the school.

Incidents will be managed through the appropriate safeguarding, behaviour, anti-bullying or staff procedures.

25. Online Abuse or Harassment of Staff

The school does not consider online abuse, intimidation or harassment of staff to be an acceptable part of working in education.

Concerns involving:

- abusive messages;
- threatening posts;
- defamatory content;
- impersonation;
- doxxing;
- malicious sharing of personal information;
- persistent unwanted contact; or
- targeted online campaigns

will be taken seriously.

The DfE published specific online-safety guidance for school staff in July 2026, recognising online safety as part of both professional conduct and personal security.

Where appropriate, the school may preserve evidence, report content to the relevant platform, seek advice, restrict communication channels or involve external agencies.

26. Parents and Carers

Parents and carers are encouraged to model responsible online behaviour.

The school asks parents/carers to:

- communicate respectfully about pupils, families and staff;
- raise concerns directly with the school rather than through social media;
- avoid posting material that identifies or compromises other children;
- respect the privacy of pupils appearing in photographs taken at school events;
- consider the impact of sharing images and information about their own children;
- follow age restrictions and parental controls where appropriate; and
- speak to the school where they have an online-safety concern.

27. Parent WhatsApp and Other Private Groups

The school recognises that parents may establish private WhatsApp, Facebook or other messaging groups.

Unless explicitly established and administered by the school, these are not official Wittersham communication channels and the school does not control their content.

Parents/carers are encouraged to use such groups respectfully and not to:

- discuss individual children inappropriately;
- share confidential information;
- make allegations about children, families or staff;
- share photographs of other children without appropriate permission; or
- use groups as a substitute for raising concerns directly with the school.

Safeguarding concerns arising from private groups should be reported to the school.

28. Reporting Concerns

Pupils should be encouraged to tell a trusted adult whenever something online:

- frightens them;
- worries them;
- makes them uncomfortable;
- asks them to keep inappropriate secrets;
- requests personal information or images; or
- involves bullying, threats or inappropriate contact.

Staff must report safeguarding concerns immediately through the school's safeguarding procedures.

29. Concerns About Staff

Any concern regarding a member of staff's online conduct must be reported in accordance with the school's Child Protection and Safeguarding Policy.

This includes conduct which may:

- meet the harm threshold; or
- constitute a low-level concern.

Staff do not need to determine the threshold before reporting a concern.

KCSIE 2026 makes clear that safeguarding concerns or allegations about staff, including supply staff, trainees, volunteers and contractors, must be managed through the school's safeguarding procedures.

Where a concern relates to the Headteacher, it must be reported to the Chair of Governors.

30. Responding to Incidents

Where an online or social-media incident occurs, the school will consider:

- immediate safeguarding;
- the child's welfare;
- preservation of appropriate evidence;
- whether parents/carers should be informed;
- whether content should be reported to a platform;
- behaviour or disciplinary procedures;
- pastoral support;
- whether external advice is required;
- whether Children's Social Care or the police should be involved; and
- whether the incident identifies a wider safeguarding or curriculum need.

31. Recording

Safeguarding concerns arising through social media will be recorded through the school's safeguarding recording procedures.

KCSIE 2026 emphasises that safeguarding records should include the concern, actions taken, decisions, rationale and outcomes.

Relevant screenshots or other evidence should only be retained where necessary and appropriate, and handled securely.

32. Monitoring

School-owned devices and systems may be appropriately filtered and monitored in accordance with safeguarding requirements.

Pupils and staff should have no expectation that use of school-owned systems is completely private.

Monitoring will be proportionate and undertaken for legitimate safeguarding, security and operational purposes.

33. Policy Breaches

Breaches of this policy will be considered according to the nature and seriousness of the incident.

For pupils, this may involve:

- safeguarding action;
- education and support;
- restorative work;
- parental involvement; and/or
- action under the Behaviour Policy.

For staff, breaches may be considered under:

- safeguarding procedures;
- low-level concerns procedures;
- the Staff Code of Conduct;
- disciplinary procedures; and/or
- professional conduct requirements.

Serious matters may be referred to external agencies.

34. Whistleblowing

All staff have a responsibility to raise concerns about unsafe, inappropriate or potentially harmful practice within the school. Concerns relating to safeguarding, professional conduct or the welfare of children must be taken seriously and reported promptly through the school's safeguarding, Low-Level Concerns, Managing Allegations or Whistleblowing procedures, as appropriate.

Staff should normally raise safeguarding concerns with the Headteacher/Designated

Safeguarding Lead. Where a concern relates to the Headteacher, it must be reported to the Chair of Governors in accordance with the school's safeguarding procedures.

Staff must not allow concerns about loyalty to colleagues, fear of repercussions or uncertainty about the seriousness of an issue to prevent them from raising a genuine concern. No member of staff is expected to investigate a safeguarding concern themselves before reporting it.

Where a member of staff feels unable to raise a safeguarding concern internally, believes that their concern has not been addressed appropriately, or considers that there is an immediate safeguarding risk, external whistleblowing routes are available.

Keeping Children Safe in Education (KCSIE) 2026 identifies the NSPCC Whistleblowing Advice Line as an external route for professionals who have concerns about how child-protection issues are being handled within their organisation.

The school will support staff who raise genuine concerns in good faith and will not tolerate victimisation or detrimental treatment of an individual for raising a legitimate safeguarding or whistleblowing concern.

35. Links with Other Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policy;
- Online Safety Policy;
- Acceptable Use Policy;
- Staff Code of Conduct;
- Low-Level Concerns procedures;
- Whistleblowing Policy;
- Behaviour Policy;
- Anti-Bullying Policy;
- Mobile Phone and Personal Devices arrangements;
- Photography and Images Policy;
- Data Protection Policy;
- SEND Policy;
- RSE/PSHE Policy; and
- Complaints Policy.

36. Monitoring and Review

The Headteacher/DSL will oversee implementation of this policy.

The Governing Board will provide appropriate oversight.

The policy will be reviewed annually and sooner where:

- Keeping Children Safe in Education changes;
- regulations or guidance under the Children's Wellbeing and Schools Act 2026 are introduced;
- online-safety legislation changes;
- DfE mobile-phone guidance changes;
- new social-media or AI risks emerge;
- local safeguarding procedures change; or
- an incident identifies a need for review.

Policy adopted: September 2026

Next review: September 2027