



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



Communications, Social Media and Image Use Procedure

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Contents

1. Purpose and scope	3
2. Legal and guidance framework	3
3. Principles and responsibilities	4
4. How may we communicate?.....	5
5. How may we use social media?	7
6. How may we capture and use images and recordings?	9
7. Live video, livestreaming and remote communication.....	11
8. Website, publications and external media.....	12
9. AI-generated and manipulated media, smart devices and wearables	13
10. What do we do when something goes wrong?.....	13
11. Training, assurance and review	15
Appendix A. Local communication and publication controls	16
Appendix B. Quick decision guide for staff	18

1. Purpose and scope

This procedure sets out how the setting will manage electronic communications, social media, photographs, video, audio and other recorded or published content in a way that protects children, supports professional boundaries and meets applicable safeguarding and data protection requirements.

It applies to staff, children and learners, governors or trustees, volunteers, contractors, visitors and third-party providers where their communication, recording or publication activity is connected with the setting.

It covers:

- approved organisational email, messaging, learning platforms and other setting-authorized communication systems;
- communication with children, learners, parents and carers;
- official and personal use of social media where this affects the setting, professional conduct or safeguarding;
- photographs, video, audio, livestreams, video calls and recordings;
- websites, newsletters, prospectuses, digital displays, promotional material and external publications;
- AI-generated or manipulated images, video and audio, including deepfakes and cloned voices;
- AI-enabled smart devices and smart wearables, including smart glasses and wearable cameras, where they can capture, record, transcribe, transmit or generate content; and
- remote or off-site communication undertaken for setting business.

Detailed rules about mobile phones and personal devices sit in the Mobile Phone and Personal Device Policy. Detailed AI controls sit in the AI and Emerging Technology Procedure. This document addresses those technologies only where they are used to communicate, record, publish or share content.

2. Legal and guidance framework

Keeping Children Safe in Education (KCSIE) requires schools and colleges to address acceptable use of technologies, staff/pupil relationships and communications, including social media, within the staff behaviour policy or code of conduct. KCSIE 2026 comes into force on 1 September 2026.

Images, video and audio in which an individual can be identified are personal data. Their capture, storage, sharing and publication must therefore comply with UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, where those laws apply.

Data protection law does not require one universal lawful basis for all school photography. The setting must identify and communicate the lawful basis that applies to each purpose. Consent may be appropriate in some circumstances, but it is not automatically the correct lawful basis for every photograph or video.

Where the statutory Mobile Phones in Schools guidance applies, schools should prohibit pupil use of mobile phones throughout the school day and may include other communications and smart technology with similar functionality within the scope of their policy.

3. Principles and responsibilities

The setting will apply the following principles:

- Professional boundaries apply online and offline. Technology does not change the standard of conduct expected of staff.
- Official setting business will use approved organisational accounts, devices and communication channels.
- Communication involving children and learners should be transparent, purposeful, open to appropriate scrutiny and limited to legitimate educational, pastoral or organisational activity.
- Safeguarding concerns take priority over reputational or communications considerations.
- Images and recordings will be captured and used only for identified purposes and with appropriate safeguarding, privacy and data protection controls.
- Official publication and social-media activity will be authorised, securely administered and monitored.
- Children, learners and families will be given clear information about how official images and recordings may be used and how to raise concerns.
- AI-generated or manipulated media will be treated according to the underlying safeguarding, conduct, fraud, privacy or reputational risk.
- Controls will take account of SEND, accessibility, reasonable adjustments and legitimate use of assistive technology.

The Roles and Responsibilities Schedule identifies the relevant governance, leadership, DSL, DPO, IT and staff responsibilities. Technical administration does not replace

safeguarding or leadership accountability.

4. How may we communicate?

4.1 Approved organisational channels

Staff must use setting-authorised organisational accounts and communication systems for setting business with children, learners, parents and carers. The procedure deliberately does not name individual products so that local approved systems can change without requiring the procedure to be rewritten. Please also refer to the Staff Acceptable Use Agreement (11a) for further guidance on pre-existing relationships with parents/ carers (e.g. family members.)

Approved channels currently include:

- School email accounts
- The school's approved parent communication platform(s)
- The school telephone system
- The school website and other school-managed communication platforms

The Headteacher/DSL is responsible for authorising approved communication channels and, where appropriate, delegates day-to-day management of communication systems to the School Business Manager/DDSL.

The list of approved communication channels is reviewed annually and whenever new systems are introduced.

As a minimum:

- staff must not use personal email accounts, personal telephone numbers, personal messaging accounts or personal social-media accounts for routine communication with children, learners, parents or carers;
- staff must not share personal contact details with children or learners;
- communication should normally take place at reasonable times and in accordance with local expectations about work-life balance and emergency contact;
- messages should be professional, factual and capable of being understood if later reviewed by a manager, DSL, parent or other appropriate person;
- sensitive or personal information must be communicated using an approved method appropriate to the level of risk and the setting's data-protection and cyber-security arrangements;
- staff must not bypass setting communication systems because another channel is

- quicker or more convenient; and
- where a message raises a safeguarding concern, staff must follow the safeguarding reporting route rather than relying on the communication platform alone.

4.2 Communication with children and learners

Communication must have a clear educational, pastoral, safeguarding or organisational purpose.

- Staff should not request unnecessary personal information from children or engage in communication that creates secrecy, dependency or blurred professional boundaries.
- One-to-one electronic communication must remain professional and, where appropriate, visible or recoverable within the authorised system.
- Staff should not add, follow, friend or privately message current pupils or learners through personal social-media accounts.
- Contact with former pupils or learners should use appropriate official alumni, professional or organisational routes where ongoing contact is legitimately required.

KCSIE requires staff/pupil relationships and communications, including social media, to be addressed through staff behaviour arrangements. It does not prescribe a universal rule for every pre-existing personal relationship. As a local safeguarding control, any unavoidable pre-existing family, social or community relationship that could conflict with these expectations must be declared to the headteacher/principal/manager and DSL and managed under the Staff Behaviour / Code of Conduct.

4.3 Communication with parents and carers

- Staff will use organisational accounts and approved systems for communication with parents and carers.
- Personal social-media accounts must not be used for setting communication with parents or carers.
- If a parent or carer contacts a member of staff through a personal account, the staff member should not continue the conversation there; they should preserve the relevant information, move communication to an approved route where appropriate and report the contact if it creates a safeguarding or professional-boundary concern.
- Mass or group communications must protect recipients' personal information and use approved distribution arrangements.
- Communications about safeguarding matters must follow the Child Protection and Safeguarding Policy and the Incident Response Procedure.

5. How may we use social media?

5.1 Personal social media

Staff are entitled to a private life, but personal social-media use must remain compatible with professional obligations, confidentiality and safeguarding responsibilities.

- Staff must not publish or discuss confidential setting information, pupil information, safeguarding information, images obtained through work, or information about families or colleagues where they are not authorised to do so.
- Staff should use privacy and security settings appropriately and understand that content may be copied, shared or made public beyond the intended audience.
- Staff must not present personal views as the official position of the setting.
- Staff should consider whether public posts, images, location information or other online activity could undermine professional boundaries or confidence in their professional role.
- Concerns about a staff member's online conduct must be managed through the Staff Behaviour / Code of Conduct, allegations or low-level concerns arrangements as appropriate.
- Any unavoidable pre-existing relationship that creates contact with a current pupil or parent through personal social media must be declared and managed through the local staff-conduct arrangements rather than treated as an informal exception.

5.2 Official social-media accounts

The setting may operate official social-media accounts only where their purpose has been authorised and the account is subject to clear ownership, secure administration and moderation arrangements.

- Official accounts must be created and managed using organisational contact details and authorised accounts.
- The setting must identify an accountable owner and authorised administrators.
- Access must be secured in accordance with the Cyber Security and Account Management Standard, and the setting must be able to recover or transfer administrative access when staff leave or are absent.
- Content published on behalf of the setting must be accurate, professional and consistent with safeguarding, data protection, copyright, equality and confidentiality requirements.
- Where practicable, higher-risk or sensitive public communications should be subject

to an appropriate second-person check before publication.

- Comments, replies, tags, mentions and direct messages must be moderated in accordance with local arrangements.
- Official accounts must not be used for private or secret communication with pupils or learners.
- Any official social-media activity involving pupils must use approved arrangements and should be supervised or moderated appropriately.
- Official social media must not be the only route by which essential information is made available to families, because not all members of the community use social-media services.
- Images or recordings published through official accounts must meet the requirements in section 6.

The school's official social media presence is its Facebook page, *Alfriston Primary School*, administrated by the School Business Manager.

The Facebook page is monitored regularly. All content is approved by an authorised administrator and comply with the school's safeguarding, data protection and acceptable use policies. Inappropriate comments or messages will be removed where necessary and safeguarding concerns will be referred to the DSL.

5.3 Pupil and learner social-media use

The setting will teach safe and responsible social-media use through the curriculum and respond to harmful social-media behaviour through safeguarding, behaviour and anti-bullying arrangements as appropriate.

- The setting will not create or require accounts for children where this would conflict with the service's age requirements.
- Pupils should be taught to protect personal information, use privacy and reporting tools, recognise impersonation and scams, and seek help where contact or content causes concern.
- Online bullying, harassment, sexual harm, threats, hate, exploitation, impersonation or harmful image-sharing will be treated according to the underlying behaviour and safeguarding risk rather than simply as a 'social-media issue'.

6. How may we capture and use images and recordings?

6.1 General rules for setting-created images and recordings

Before taking or using a photograph, video or audio recording, the setting should be clear about the purpose, who will have access, where it will be stored, whether it will be published, how long it will be retained and what lawful basis applies.

- Only setting-authorized devices and systems should be used to capture or store images of children for setting purposes.
- Staff must not use personal phones, personal cameras, smart glasses, wearable cameras or other personal devices to photograph, film or record children, except under a formally authorised exceptional arrangement.
- Pupils must not use personal devices to photograph, film or record other people within the setting unless specifically authorised as part of a supervised activity.
- Images should be appropriate, dignified and relevant to the stated purpose.
- Images should not reveal unnecessary personal information, sensitive locations or information that could increase safeguarding risk.
- The setting should avoid combining a child's full name with an identifiable image in public-facing material unless there is a clear, assessed and appropriate reason.
- Images and recordings must be stored securely and access limited to those who need them.
- Deletion and retention must follow the setting's retention arrangements and the purpose for which the image was created.

6.2 Lawful basis, consent, permission and objections

Where an identifiable image or recording is used for official setting purposes, data protection law applies. The setting must determine the correct lawful basis for the particular use and provide appropriate privacy information.

- Consent is one possible lawful basis but is not automatically required or appropriate for every image or recording.
- Where consent is the lawful basis, it must meet the requirements of data protection law and withdrawal must be as easy as giving consent.
- Where another lawful basis is used, the setting should still consider objections or opt-out arrangements where appropriate, particularly for promotional or public-

facing use.

- The child's age, understanding and rights should be considered when determining whether the child or parent/carer should exercise the relevant data-protection choices.
- The DPO or data-protection lead should advise where the lawful basis or level of risk is unclear.

6.3 Publication and promotional use

Images used on the website, official social media, newsletters, prospectuses, digital displays, promotional material or external publications must be approved for that purpose and used consistently with the privacy information provided.

- The setting should use the minimum identifying information necessary.
- Images must not be reused for a materially different purpose without checking whether the existing lawful basis and privacy information still support that use.
- Where an image is supplied to an external organisation, the setting should be clear about the intended use and whether the external organisation becomes responsible for its own processing.
- Requests to remove or stop using an image should be considered promptly in accordance with the applicable lawful basis and information-rights framework.

6.4 Parents and carers photographing or filming events

As a local safeguarding control, the default position is that parents, carers and other audience members are not permitted to photograph, film, audio-record or livestream setting events.

- This rule is not presented as a requirement of data protection law. The ICO explains that purely personal or household photography may fall outside data-protection law, but settings may establish their own event rules for safeguarding and child-protection reasons.
- The restriction should be communicated clearly before and at the event.
- The setting may arrange its own authorised photography or recording where appropriate and lawful.
- Any exceptional event-specific permission for audience photography must be explicitly authorised by the setting in advance and communicated with clear conditions.
- Staff should respond proportionately where a person does not follow the event rule, taking account of safeguarding, safety and the setting's visitor arrangements.

7. Live video, livestreaming and remote communication

Live video and remote communication may be used where they support education, pastoral work, meetings, intervention or community engagement. The safeguards below modernise, but do not weaken, the controls in the existing online-safety policy.

7.1 General live-session controls

- Only setting-approved platforms and organisational accounts may be used.
- The platform and intended use should be risk assessed, including chat, recording, screen-sharing, participant admission, background effects and pupil-camera controls.
- Staff must use organisational devices and contact details wherever practicable and must not use personal accounts to run sessions.
- Sessions should be planned and scheduled at appropriate times.
- Staff conduct, language and appearance must remain consistent with the Staff Behaviour / Code of Conduct.
- Pupils should participate from an appropriate location and should not be encouraged to expose private household information unnecessarily.
- Participants must not record sessions unless recording has been explicitly authorised and the data-protection arrangements have been established.
- A member of staff must moderate pupil interaction and respond to inappropriate behaviour or safeguarding concerns promptly.
- Filtering and monitoring may not prevent inappropriate content appearing in a live interaction; active professional supervision remains essential.

7.2 Two-adult safeguard and one-to-one sessions

As a local safeguarding control, interactive live sessions with children should normally have two adults present or otherwise involved in accordance with the setting's approved model. This preserves the safeguard contained in the existing policy.

- The second adult may provide safeguarding, behaviour or technical support and does not need to be a curriculum specialist.
- Where staff are remote, both adults should be present in the virtual session before pupils are admitted where the local model requires this.
- A one-to-one session may be appropriate for counselling, therapeutic, SEND,

pastoral or other specialist work where confidentiality or professional practice makes a two-adult model unsuitable.

- Such one-to-one arrangements must be risk assessed and approved by the appropriate senior leader, with parental involvement or agreement where required by the setting's safeguarding model and the nature of the service.
- The setting must not assume that recording a one-to-one session is automatically required or automatically lawful. If recording is proposed, the purpose, lawful basis, access, retention and safeguarding implications must be determined before recording begins.

7.3 External livestream providers

- Staff should check the suitability of live content and the safeguarding arrangements of the provider before directing pupils to participate.
- The setting should understand whether pupils can appear on camera, use chat, direct-message, upload content or interact with people outside the setting.
- For live events involving pupil participation, an appropriate member of staff should monitor content and interaction.
- Where an external provider runs repeated or ongoing sessions, leaders should obtain proportionate assurance about safeguarding and moderation arrangements.

8. Website, publications and external media

The setting's website, newsletters, prospectuses, digital displays and other publications must be managed as official communications.

- Published information must be accurate, accessible and consistent with data protection, copyright, intellectual-property, safeguarding and confidentiality requirements.
- Personal contact details for individual staff or pupils should not be published where organisational contact details are appropriate.
- Administrative access to websites and publication systems must be secured under the Cyber Security and Account Management Standard.
- Safeguarding and online-safety information for the community should be made accessible through appropriate official channels.
- Images and recordings used in publications must comply with section 6.
- Media requests involving children should be coordinated through an authorised senior lead and should ensure children and parents/carers understand the intended context and publication arrangements where relevant.

9. AI-generated and manipulated media, smart devices and wearables

This procedure applies equally where communication or recorded content is created, altered, summarised, transcribed or transmitted using AI.

- Deepfakes, cloned voices, synthetic images, AI-altered photographs and AI-generated video or audio must not be used to impersonate, humiliate, sexualise, deceive or harass another person.
- AI-generated or manipulated sexual imagery involving a child must be treated as a safeguarding concern and managed through the Incident Response Procedure and AI and Emerging Technology Procedure.
- Staff must not use AI to create synthetic communications that could mislead a pupil, parent, colleague or member of the public about who authored or approved the message.
- AI-enabled smart glasses, wearable cameras, voice assistants and smart wearables must be treated as recording/communications devices where they can capture, transcribe, transmit, identify or generate content.
- Personal smart wearables must not be used by staff to record children or confidential setting activity.
- Where an AI-enabled wearable or assistive device is needed for accessibility or reasonable adjustment, the setting should assess the actual recording, privacy, safeguarding and security risks rather than applying a blanket prohibition.
- Use of AI to edit or enhance official images must not materially misrepresent a child, event or setting activity without a legitimate, transparent and approved reason.

10. What do we do when something goes wrong?

Concerns should be routed according to the underlying harm. Staff should not attempt to resolve a safeguarding, staff-conduct, cyber-security or data-protection incident solely as a communications problem.

Concern	Primary route	Immediate principle
A pupil sends a concerning message, image or disclosure	DSL / DDSL	Preserve relevant information where safe, do not conduct unnecessary investigation, and follow the Incident Response Procedure.

Concern	Primary route	Immediate principle
A parent or pupil contacts a staff member's personal account	DSL / DDSL if safeguarding or boundary concern	Do not continue the conversation on the personal channel; move to an approved route where appropriate and record/report concerns.
A staff member's social-media conduct raises concern	Headteacher / SBM	Use Staff Behaviour / Code of Conduct, low-level concern or allegation procedures as appropriate.
An official account is compromised or impersonated	IT / cyber route Headteacher / SBM	Secure the account, preserve evidence, assess communications impact and involve DSL/DDSL/DPO where relevant.
An image or recording is published incorrectly	DPO / relevant senior lead	Contain further sharing where possible, assess the lawful basis and any personal-data breach, and respond to safeguarding implications.
A parent/carers photographs or films an event despite the local prohibition	Headteacher / SBM	Apply the communicated event rule proportionately and consider safeguarding or visitor-management concerns.
A deepfake, cloned voice or synthetic image is used to target a child or staff member	DSL / DDSL; IT/DPO as relevant	Treat according to the harm: safeguarding, harassment, fraud, staff conduct, cyber security or data protection.
A personal smart wearable records or transmits confidential activity	DSL / DDSL / DPO	Stop or contain the activity, preserve relevant information and assess safeguarding/privacy implications.
Harmful comments or messages appear on an official social-media account	Authorised account administrator (SBM) / Headteacher	Moderate in accordance with the account rules; preserve evidence where needed and escalate safeguarding or harassment concerns.

11. Training, assurance and review

Staff induction and updates should cover approved communication channels, professional boundaries, social-media expectations, image use, live video and reporting routes.

Staff authorised to manage official social-media or publication systems should understand account security, moderation, data protection and escalation arrangements.

Staff taking or publishing images should understand the local lawful-basis and privacy-information arrangements rather than relying on an assumption that 'consent is always required'.

Leaders should periodically review official accounts, authorised administrators, image/publication arrangements and remote-communication controls.

The procedure should be reviewed after significant safeguarding, reputational, privacy or account-security incidents and when new technologies introduce materially different communication or recording capability.

Reviews should check consistency with the Core Online Safety Policy, AI and Emerging Technology Procedure, Mobile Phone and Personal Device Policy, Cyber Security and Account Management Standard, Data Protection Policy and Staff Behaviour / Code of Conduct.

Appendix A. Local communication and publication controls

Control	Local position
Approved organisational communication channels	• School email accounts • The school's approved parent communication platform(s) • The school telephone system • The school website and other school-managed communication platforms
Role authorised to approve new communication systems	Headteacher
Official social-media accounts	Facebook: Alfriston Primary School
Authorised social-media administrators	Headteacher and School Business Manager
Moderation and direct-message arrangements	The Facebook account is monitored regularly by authorised administrators. Inappropriate comments may be hidden or removed. Direct messages are reviewed by authorised administrators and responded to through approved school communication channels where appropriate. Safeguarding concerns are referred immediately to the DSL.
Authorised devices for staff photography/video	School-owned devices only, including school iPads and other authorised school equipment. Personal devices must not be used unless specifically authorised by the Headteacher in exceptional circumstances.
Public-facing image/privacy arrangements	Publication of pupil images is managed in accordance with parental consent records, the school's Privacy Notice and Data Protection Policy. Consent records are maintained through the school's management information system.
Parent/carers event photography	Not permitted by default unless an event-specific exception is authorised and communicated
Approved live-video / remote-communication route	Microsoft Teams using school-managed accounts.
Local two-adult live-session model	Live sessions should normally be conducted with two members of staff present or with another member of staff able to access and monitor the session. Any exceptions

Communications, Social Media and Image Use Procedure

Control	Local position
	(e.g. SEND support or pastoral meetings) must be risk assessed and approved by the Headteacher.
Media / press contact	Headteacher
DPO / Data Protection Lead	School Data Protection Officer
DSL / safeguarding reporting route	Designated Safeguarding Lead (Lindsey Hudson - HT) and Deputy Designated Safeguarding Lead (Tanya Fitzgerald - SBM)

Appendix B. Quick decision guide for staff

If...	Staff should...
I need to contact a pupil or parent.	Use an approved organisational account or system. Do not use a personal account or personal telephone number.
A pupil or parent has contacted my personal social-media account.	Do not continue the conversation there. Preserve relevant information, move to an approved route if appropriate, and report any safeguarding or professional-boundary concern.
I want to post something on an official social-media account.	Check that you are authorised, the content is appropriate, any image use is approved for that purpose, and any required moderation/second-person check is complete.
I want to photograph or film pupils.	Use an authorised setting device and check the purpose, privacy/lawful-basis arrangements and safeguarding suitability. Do not use your personal phone or wearable.
A parent wants to photograph a school event.	The default local position is no photography, filming, audio recording or livestreaming by audience members unless the setting has explicitly authorised an exception.
I want to run a live video session.	Use an approved platform and organisational account; apply the local two-adult and risk-assessment arrangements; do not assume the platform's technical controls replace supervision.
I want to record a video call.	Do not record automatically. Establish the purpose, lawful basis, safeguarding need, access and retention before recording.
I need a smart wearable or AI-enabled device for accessibility.	Do not apply a blanket ban. Refer the use for proportionate safeguarding, privacy, security and reasonable-adjustment assessment.
I see a deepfake or synthetic image involving a child.	Treat it according to the underlying safeguarding risk and report to the DSL; do not investigate unnecessarily.
I am unsure whether a communication or image is appropriate.	Do not publish or send it until you have checked with the relevant manager, DSL, DPO or communications lead.