



SAFE START SCHOOL

WILLPOWER-INITIATIVE-SUCCESS-EMPATHY-RESPECT

Online Safety Policy

October 2026

To be reviewed October 2027

Reviewed by: Grace Speakman

Verified by: Rachel Pilling

Purpose scope and framework

Online safety is part of safeguarding, learning and daily school practice. Safe Start School aims to prevent harm, help pupils use technology confidently and provide clear routes for reporting and responding. This policy applies to pupils, staff, governors, volunteers, contractors and visitors using school systems, including off-site and remote use. Online harm outside school will also be addressed where it affects pupils' safety, wellbeing or education.

The policy reflects Keeping children safe in education 2026; current DfE filtering and monitoring standards; Teaching online safety in schools; statutory relationships and sex education guidance applicable to independent schools; Prevent guidance; Searching, screening and confiscation guidance; UKCIS advice on sharing nudes and semi-nudes; and relevant education, equality, criminal and data protection law. It complements safeguarding, behaviour, anti-bullying, staff conduct, smart devices, photography, data protection, complaints and remote education policies.

Children means those under 18. Pupils aged 18 or over remain entitled to support, with adult safeguarding, consent and capacity considered where relevant. SEND or emotional and behavioural needs must not be taken to mean that a pupil cannot understand risk, but teaching and support must be adapted to their individual understanding and communication needs.

Risks and prevention

The school considers four connected areas: content such as pornography, hate, extremist material, self-harm material and misleading information; contact such as grooming, coercion, exploitation and unwanted approaches; conduct such as bullying, harassment, harmful image sharing and impersonation; and commerce such as gambling, scams, phishing and exploitative purchases.

Risk assessment also considers misogyny, discriminatory abuse, harmful influencers, gaming and livestreaming, location sharing, sexual extortion, criminal exploitation, manipulative online communities, AI companions and synthetic images. A single post may cause repeated harm through copying and sharing. An apparently consensual interaction can involve pressure or exploitation; staff must not dismiss abuse as banter or normal teenage behaviour.

Roles and responsibilities

The proprietor has strategic oversight and receives assurance on online safeguarding and technical protection. The Headteacher is the responsible senior leader, assigns resources and checks implementation. HR maintains induction and training records. Roles are allocated by responsibility rather than assuming the school has an internal IT department.

The DSL, supported by trained deputies, leads online safeguarding, reviews relevant alerts and reports, records concerns on CPOMS, coordinates referrals and pupil support and reports anonymised themes to leaders and the proprietor. Current DSL names and contact arrangements are set out in the Safeguarding and Child Protection Policy and displayed in school; staff must use these current details.

The designated IT lead or contracted IT provider installs and maintains technical protections, supplies reports, checks coverage, investigates faults and records remedial work. IT does not replace the DSL's safeguarding judgement. Staff supervise online activity, check teaching resources, follow professional boundaries and report concerns immediately. Pupils and families are encouraged to report mistakes or worries promptly without fear of blame.

Filtering and monitoring arrangements

Filtering limits access to harmful content; monitoring identifies activity that may need attention. Neither is complete protection or a substitute for supervision. The Headteacher, DSL and IT provider will maintain a written schedule naming systems, responsible people and deputies, devices and locations covered, report and alert routes, checking frequency, response arrangements, retention and known limitations.

The schedule must distinguish school networks, school-managed devices used elsewhere, guest access, cloud platforms and personal mobile data. Staff must not assume off-site devices, AI conversations, encrypted apps or mobile hotspots are covered. Coverage will be verified with the provider and gaps addressed through technical changes, restrictions or additional supervision. Do not permit unsupervised pupil access where protection is absent or a significant fault makes access unsafe.

Designated staff will check relevant alerts and reports each school day, with deputies covering absence. Urgent alerts require immediate safeguarding action when received; do not wait for a routine report or meeting. The school will document what happens outside staffed hours and explain limitations to families; it must not claim continuous monitoring unless this has been commissioned and verified. Families should use emergency services for immediate danger rather than rely on an online alert being seen.

Record alert time, review, risk judgement, action, referral, support and closure in the appropriate safeguarding or technical record. Distinguish technical faults and false positives from safeguarding concerns. A blocked search can still indicate risk. Repeated concerns, attempts to bypass protection and unresolved alerts must be reviewed for patterns. Sensitive alert information must not be circulated unnecessarily.

SLT, the DSL and IT support will review effectiveness at least once each academic year, with proprietor oversight, and after significant changes or incidents. Record tests using safe recognised tools across relevant devices, user groups and locations, actions, owners and completion dates. Check protection against illegal and terrorist content, age-inappropriate content and evasion methods without accessing illegal material. Do not overblock legitimate learning or support resources; requests to change filtering require authorised safeguarding and technical review.

Consider age, SEND, individual vulnerabilities, staff use, remote education and dynamic or AI-generated content when choosing and testing systems. Users and families will be told what is monitored, why, its scope and reporting routes through accessible notices and agreements. Processing, access and retention must meet the Data Protection Policy; an acceptable-use signature does not replace a lawful basis.

Teaching pupils and working with families

Online safety is taught through PSHE, relationships and sex education, digital learning, relevant subjects and planned awareness activities. Staff will revisit learning, use accessible examples and check understanding through discussion, scenarios and supported practice. Content will reflect pupils' developmental needs, experiences and post-16 preparation for adulthood, with individual work where required.

Teaching covers healthy relationships and consent; privacy and digital footprints; safe passwords and account security; gaming, purchases and scams; misinformation and source checking;

reporting and blocking; safe help-seeking; and responding to pressure, threats or unwanted content. Pupils will learn that an online identity may be false and that AI outputs may be convincing but inaccurate, biased or harmful. They will be taught not to create or share sexualised images, including synthetic images of others, and that adults will help if something has happened.

Avoid frightening pupils into silence or suggesting they are responsible for exploitation. Explain legal risks accurately without implying every child who reports an image incident will be prosecuted. Pupils will practise telling a trusted adult, including when they have broken a rule. Provide alternative reporting methods for pupils who cannot easily explain verbally.

Families will receive information about school systems, platforms, expected contacts, reporting routes and relevant emerging risks through school communications and the website. Encourage safe account settings, age-appropriate access, trusted conversations and awareness of mobile data and hotspots. For adult pupils, involve families consistently with the pupil's rights and wishes. The school will seek pupil and family feedback to improve provision.

Devices acceptable use and professional boundaries

Use school systems for authorised education and work. Individual logins must be used where provided; supervision does not mean sharing staff passwords. Do not bypass filtering, use unauthorised VPNs or hotspots, install unapproved software or access another person's account. Protect records, lock screens and report phishing, lost devices and suspected compromise immediately.

Pupils hand in phones at reception and follow the current smart devices policy throughout the school day. Smart watches, earbuds and other connected devices follow that policy. Any exceptional access needs Headteacher authorisation and an individual assessment, including applicable medical, disability, reasonable-adjustment and EHCP requirements. Routine lesson activities should use approved school devices. Personal mobile data does not make unsafe use acceptable; staff must act on breaches and concerns.

Staff must use approved school accounts for pupil contact and follow staff mobile phone and photography rules. Do not use personal social media to contact current pupils, share personal contact details unnecessarily or photograph pupils on personal devices. Any exceptional safeguarding communication must follow authorised arrangements and be recorded. Report attempted inappropriate contact or boundary concerns rather than managing them privately.

Only authorised staff may publish on official school accounts. Follow current image permissions, safeguarding restrictions and data protection rules. Do not post sensitive records, pupil locations or identifying details that create risk. Visitors use authorised guest access and follow school photography rules. Refusal to sign an agreement is discussed and recorded; it does not remove the school's safeguarding responsibilities.

Remote education AI and external provision

Use approved remote-learning platforms, school accounts, controlled invitations and appropriate access settings. Explain arrangements to pupils and families, use professional locations and backgrounds and assess the safeguards for any one-to-one session. Recording or livestreaming requires separate approval, a lawful basis, clear information and retention arrangements; it is not authorised by general photo consent. Provide a clear route for reporting concerns during remote work.

Before introducing AI tools, the Headteacher, DSL, data protection lead and IT support must assess age terms, accessibility, moderation, privacy, supplier use of data, technical coverage and human oversight, using DfE product safety standards. Do not assume an ordinary web filter can see or moderate an AI response. Pupils may use only approved tools for an agreed learning purpose. Staff must check outputs and not use AI as a substitute for safeguarding judgement.

Do not enter identifiable pupil, family or staff information, images, voices or confidential records into public or unapproved AI services. Do not generate harmful sexualised content, impersonate others or use unapproved bots to communicate with pupils. Suspected AI image abuse or exploitation receives the same safeguarding attention as other online harm.

Where pupils attend alternative provision, the school will agree online safety responsibilities, reporting routes, supervision and filtering arrangements with the provider and check them through quality assurance. School responsibility does not end because a pupil learns elsewhere. Cyber security and recovery follow the Data Protection Policy and Business Continuity Plan. School files are currently in Google Drive without a separate school-maintained backup; planned Microsoft backup arrangements must not be described as operational until implemented and tested. Leaders will record the gap and pursue interim protection with IT support.

Reporting concerns and initial action

Tell the DSL or a deputy immediately about suspected grooming, exploitation, sexual harassment, image abuse, threats, radicalisation, self-harm risk or other safeguarding concerns. If they are unavailable, follow the safeguarding escalation route and contact children's social care or police directly where necessary. Call 999 for immediate danger. Do not delay action for a form, parent permission or a scheduled alert check.

Listen, reassure and avoid blame. Establish immediate safety without conducting a detailed investigation. Record facts, dates, relevant words, accounts and URLs without copying illegal imagery. Preserve appropriate non-sexual evidence securely, restrict harmful access and obtain DSL advice on blocking and reporting. Do not confront a suspected abuser or communicate in a way that may increase risk.

The DSL assesses risk, support, parental contact and agency referrals, and records reasons. Inform parents unless doing so may increase risk or prejudice protection. For concerns about adults, use allegations and low-level concerns procedures, with LADO advice where appropriate. Criminal or child protection enquiries take priority over internal fact-finding. Data breaches go promptly to the DPO and IT support as well as the DSL where relevant.

Sexual imagery sexual extortion and harmful content

Report all nude, semi-nude or sexualised image concerns involving under-18s immediately to the DSL, including digitally altered or wholly AI-generated images. Staff must not request, deliberately view, screenshot, print, save or forward suspected child sexual imagery or ask a pupil to send it. If accidentally seen, stop viewing and report; do not circulate it as evidence. Secure a relevant device lawfully, avoid further handling and obtain DSL advice; do not delete potential evidence.

The DSL will use current UKCIS guidance for an initial review, risk assessment, support and referrals. Immediate referral to police and/or children's social care is required where the guidance criteria apply, including adult involvement, coercion, blackmail, grooming, exploitation or concerns about capacity to consent, sexual acts involving a child under 13, developmentally unusual or violent sexual acts, or immediate risk of harm. Do not promise that every incident will stay within

school or that every incident automatically requires criminalisation. Any exceptional viewing must be justified, authorised and recorded under the guidance, not carried out by ordinary staff for reassurance.

For sexual extortion, reassure the pupil that they are not to blame. Do not advise paying, sending further images or negotiating with the offender. Obtain police and safeguarding advice, agree safe contact and reporting steps and assess immediate emotional safety. Use approved removal routes such as Childline/IWF Report Remove for eligible under-18 cases, with professional support. Never seek out illegal material to confirm a report. Do not share operational details publicly.

Cyberbullying searches and proportionate action

Respond to cyberbullying whether on school platforms or elsewhere. Consider repeated exposure, power imbalance, discrimination, sexual abuse and impact, even where there was only one original upload. Support the pupil, assess wider safeguarding risks, document appropriate evidence and take proportionate action under the behaviour policy with SEND and individual circumstances considered. Do not make mediation the default where there is abuse, coercion or a safety risk.

Only the Headteacher and staff specifically authorised for the relevant search may exercise statutory search powers. Follow current DfE guidance and the school's behaviour/search procedures, considering grounds, urgency, privacy, age, SEND, cooperation, witness requirements, recording and parental notification. Confiscating a device does not give every staff member unrestricted authority to inspect messages, images or cloud accounts. School staff must not conduct strip searches.

Device examination requires a lawful basis and good reason under the applicable powers. Deletion is not routine and must follow the legal conditions and safeguarding advice. Never delete material suspected to be evidence of an offence; obtain police advice and hand over a device as required. Suspected sexual images follow section 9. Record the reason, authorisation, actions, outcome and support. Concerns about a search may be raised through the complaints procedure.

Training review and assurance

Staff receive online safeguarding and filtering/monitoring responsibilities at induction, appropriate training and at least annual safeguarding updates, with further briefings as risks change. DSL and deputy training follows the Safeguarding Policy, including formal updates at least every two years and knowledge refreshed at least annually. Leaders and governors receive training appropriate to their oversight roles. Agency staff and visitors receive relevant instructions before access.

The DSL will report themes, responses, unresolved risks and training needs to the Headteacher and proprietor at least termly, with urgent escalation outside that cycle. Review the policy and online risk assessment annually, using pupil feedback, incidents, AP quality assurance and technical review findings. Keep evidence of actions and closure. The policy must describe verified arrangements; gaps require recorded action rather than an unsupported assurance of safety.

Key sources: KCSIE 2026; DfE Filtering and monitoring core standard and Generative AI product safety standards; DfE Searching screening and confiscation; UKCIS Sharing nudes and semi-nudes, 2024; and the school policies named in section 1. The appendices form part of this policy.

Appendix 1 Pupil acceptable use agreement

Pupil name: _____ Class: _____ Date: _____

Staff will explain these rules in a way I understand and help me use technology safely.

- I will use school devices and accounts for agreed learning and follow adult instructions.
- I will keep passwords private, use my own account where provided and log off when finished.
- I will treat others respectfully and not bully, threaten, impersonate or share private information.
- I will not make, request or share sexual images, including fake images. If something happens, I will tell a trusted adult and will not forward it.
- I will not bypass filters, use unauthorised hotspots or VPNs, install software or use AI tools without permission.
- I will not share personal details or arrange an online contact meeting without safe adult support.
- I will hand in my phone and follow the smart devices and photography rules.
- If content, contact, a request for money or an online message worries me, I will tell an adult promptly, even if I have broken a rule.

The school explains and monitors authorised use for safety. Filters cannot prevent every risk. Staff will support me and respond fairly to misuse. This agreement is not consent to unlimited monitoring.

Pupil signature or agreement recorded: _____

Staff support or communication method: _____

Parent/carer acknowledgement, where appropriate: _____

Date: _____

Appendix 2 Staff and visitor acceptable use agreement

Name and role: _____

- Use only authorised systems, accounts and software; protect passwords and use required security controls.
- Keep professional boundaries and contact pupils through approved school routes.
- Protect personal data and use images only under the Photography and Data Protection Policies; never use personal devices for pupil photographs.
- Supervise pupil activity, check resources, understand monitoring limitations and report alerts or faults.
- Do not access or share illegal, discriminatory, abusive or unauthorised material, bypass protections or upload confidential information to unapproved AI tools.
- Report safeguarding concerns immediately to the DSL and security/data incidents through the relevant routes. Do not investigate or copy suspected child sexual imagery.
- Follow these rules off site when handling school information or using school devices. Legitimate complaints, whistleblowing and safeguarding reporting remain protected.

I understand that authorised school-system use is monitored within the published scope and privacy arrangements. I have read the relevant rules and know how to obtain advice.

Signature: _____ Date: _____

Appendix 3 Parent and carer guide

Help your child understand safe and respectful online behaviour, privacy settings, age restrictions, scams, purchases and where to seek help. Talk about pressure and unsafe contact without blame. Tell the DSL or another member of staff about concerns, including incidents away from school. Immediate danger requires 999. Do not wait for the school to read a monitoring alert outside staffed hours.

Follow the smart devices and photography policies at school events. Ask before posting identifiable images of other pupils. Do not create accounts that falsely appear to be official school accounts or misuse the logo. Independent parent groups must make their status clear and protect other people's privacy. Raise school concerns through the published contact and complaints routes; reasonable criticism is not itself an online safety breach.

For bullying, retain appropriate non-sexual messages, usernames, dates and URLs, report to the school and platform and avoid retaliation. Do not copy or forward suspected child sexual images, even to school staff. Contact the DSL promptly; police or children's social care should be contacted directly where urgent protection is needed. Families should check what protection applies to home devices and mobile data.

Appendix 4 Staff incident response guide

- Protect: check immediate safety, listen and reassure; call emergency services where needed.
- Report: notify the DSL/deputy immediately for safeguarding concerns; escalate if unavailable. Notify IT and the DPO where security or personal data is involved.
- Record: log factual information and safe evidence on the appropriate restricted system. Do not request or copy sexual images.
- Assess: DSL considers risk, parental contact, referrals and support, using UKCIS guidance for imagery. Do not wait for an internal investigation where agencies need to act.
- Contain: agree safe blocking, platform reports or lawful device action; preserve potential criminal evidence and follow professional advice.
- Review: support affected pupils, check wider involvement and patterns, record decisions and actions, and confirm follow-up and closure.

Appendix 5 Social media concerns and complaints

Staff must not argue with families or pupils online or use personal accounts to defend the school. Refer concerning posts to the Headteacher; safeguarding allegations go immediately through the appropriate safeguarding route. Preserve lawful non-sexual evidence securely, assess actual harm and protect people's private information.

Distinguish a complaint or reasonable criticism from threats, harassment, discrimination, impersonation or disclosure of private information. Invite direct discussion or use the complaints process where appropriate. Do not require criticism to be removed as a condition of hearing a

complaint. Report content to a platform where its rules may be breached and seek police advice where criminal conduct is suspected; defamation is not automatically a criminal offence.

Only an authorised leader may make a public response. Do not reveal a pupil's or family's circumstances, employment details or safeguarding information to rebut a comment. Obtain advice where necessary, provide support to affected staff and pupils, and record proportionate decisions. Nothing in this policy restricts lawful reporting to regulators, police, safeguarding agencies or protected whistleblowing.