Federation of St James the Great and St John's Catholic Primary Schools

"To do our best for God, for other people" and for ourselves"

"To Love and Serve One Another"

Online Safety Policy 2026- 2027

This policy sets out how both schools protect children online, teach safe and responsible use of technology and respond to concerns. Online safety is part of safeguarding and applies to digital activity at school and to activity beyond school that affects the school community.

Review status

Updated from the September 2025 Federation policy using the supplied LGfL Online Safety Policy Template July 2026, described in the request as the Southwark template. This draft has not yet been approved

Policy owner	Designated Safeguarding Leads at both Denis O'Regan and Emily Phipps
Online safety leads	St John's: Jamie Phillips St James the Great: Justina Oduko
Deputy DSLs	Janice Babb – office@st-john.southwark.sch.uk Steffi Sadiq – office@st-john.southwark.sch.uk Jamie Phillips – office@st-john.southwark.sch.uk Jennifer Pitnat- office@stjamesthegreat.southwark.sch.uk Sally Delaney - office@stjamesthegreat.southwark.sch.uk Lil Jayawardhana - office@stjamesthegreat.southwark.sch.uk
Governor oversight	Jane McManus- governors@st-john.southwark.sch.uk

1 Aims and scope

The Federation aims to safeguard every member of its community, develop children's digital resilience, support families, enable staff to work safely and provide clear reporting procedures. Technology should support learning, inclusion and wellbeing. Expectations of respectful behaviour apply online and offline.

This policy applies to teaching, support and supply staff, governors, volunteers, contractors, visitors, pupils, parents and carers, and external groups using school systems. It covers computers, laptops, tablets, mobile phones, games consoles, cameras, microphones, smartwatches, smart glasses, other wearable or recording devices, school networks, email, cloud storage, learning platforms and AI tools. It applies to school equipment used off-site and personal technology used in a school role or in activity affecting safeguarding, professional conduct or the school community.

The policy is read alongside:

- Federation Safeguarding and Child Protection Policy,
- Behaviour and Anti-Bullying policies,
- Staff Code of Conduct,
- Acceptable use Policy
- Data protection
- AI policy.

The policy will be reviewed at least annually and when incidents, new technology or guidance require a change. Leaders will seek proportionate feedback from staff, governors, pupils and families, and review acceptable use agreements at the same time. Material changes will be communicated promptly.

2 Leadership and the four areas of risk

The DSL at each school retains lead responsibility for online safeguarding and understanding filtering and monitoring. Online safety leads support this work; their appointment does not transfer the DSL's overall safeguarding responsibility. Headteachers and governors provide leadership, resources and oversight. Appendix A sets out responsibilities.

Staff must recognise the four areas of online risk and report concerns promptly.

- Content includes illegal, harmful or inappropriate material, pornography, racism, misogyny, antisemitism, self-harm, suicide, extremism, violence, misinformation, disinformation and conspiracy theories. AI-generated material can create or amplify these risks.
- Contact includes harmful interactions, grooming, exploitation, peer pressure, advertising and contact with strangers. AI chatbots or companions can simulate relationships and provide unsafe advice.
- Conduct includes bullying, harassment, discriminatory language, sharing personal information, coercion and making or sharing sexual images, including manipulated or AI-generated imagery.
- Commerce includes gambling, scams, phishing, financial exploitation, misleading advertising and pressure to make purchases in games or apps.

The DSLs and online safety leads will use safeguarding records, filtering and monitoring information, pupil voice, parent feedback and an annual online safety audit to identify local priorities

3 Communication training and education

The policy will be available on both school websites and provided at induction, including to temporary staff and those starting during the year. Relevant expectations will be explained to visitors, contractors and external users before they access school technology.

All staff receive safeguarding training at induction that includes online safety, reporting procedures, filtering and monitoring responsibilities and professional conduct. Updates are provided as required and at least annually. Training will address emerging risks, including AI, coercion, image manipulation and recording devices. Governors receive training appropriate to their oversight role. Leaders check understanding through discussion and relevant safeguarding scenarios.

Online safety is taught progressively through Computing, Relationships Education, health education, relevant RSE content, assemblies and other subjects. Staff reinforce messages whenever technology is used, including homework. Teaching reflects children's age and development, avoids frightening or victim-blaming messages, and makes clear that children can always ask for help.

Teaching includes privacy, passwords, consent, healthy relationships, respectful communication, reporting and blocking, grooming, bullying, scams, advertising, copyright and evaluating online information. Pupils learn that search results and AI outputs may be inaccurate, biased or harmful, and that images and voices can be

manipulated. They are taught to seek help from trusted adults rather than rely on an AI companion for personal or safeguarding advice.

Staff preview resources, use guided searches where appropriate and supervise pupils' activity. They assess understanding and adapt teaching for SEND, EAL, children who have experienced abuse and others who need additional support. The curriculum is reviewed annually using local evidence and pupil feedback.

The Federation supports parents and carers through newsletters, website information, meetings and suitable awareness sessions. Families will be informed about online tasks and the services children are expected to access. Information will be accessible to families with language or additional learning needs. Staff will encourage family conversations about games, devices, privacy, age restrictions, sleep and reporting concerns.

4 Reporting and handling safeguarding concerns

Online safety concerns are safeguarding concerns, including those arising at home, during holidays or on another organisation's network. Staff must report them to the DSL without delay and record the facts, actions and outcome using the school safeguarding process. Urgent concerns require direct contact; submitting a record alone is insufficient.

If the DSL is unavailable, staff contact a deputy DSL and follow the Safeguarding and Child Protection Policy. Staff must not delay action where a child is at risk; anyone can make a referral to children's social care or the police. Call 999 where there is immediate danger.

Staff listen calmly, reassure the child, avoid blame and do not promise confidentiality. They record the child's words and necessary factual details, avoid leading questions and leave investigation to safeguarding professionals. The DSL assesses immediate safety, support needs, referrals and the risk to other children. Parents are normally informed unless this could increase risk or prejudice an investigation; the DSL seeks advice from the relevant agencies where necessary.

Concerns about staff conduct, including low-level concerns, are reported to the headteacher under the staff allegations procedure. Concerns about the headteacher go to the Chair of Governors or the alternative named in the safeguarding policy. The appropriate case manager consults the LADO when required. The school complaints process does not replace safeguarding escalation. Staff can use the applicable whistleblowing route if concerns are not addressed.

The DSL coordinates support and, where appropriate, referrals to children's social care, police, CEOP or Prevent. Technical faults are also reported to the IT provider, but technical reporting must not replace reporting a safeguarding concern to the DSL. Leaders review incidents for lessons, support and curriculum changes; sanctions are proportionate and must not discourage disclosures.

The Federation requires immediate reporting of suspected child sexual abuse, including online and non-contact abuse. Leaders will check commencement and statutory guidance for the new reporting duty in the Crime and Policing Act 2026 and update procedures and training before it takes effect. Outside school hours and during closure, parents and pupils should not assume school messages or technical alerts are continuously monitored. Immediate danger must be reported to 999 and urgent safeguarding concerns to the appropriate statutory service

Sharing nudes and semi nudes and AI generated sexual imagery

Any disclosure or discovery of sexual imagery involving a child is reported immediately to the DSL. Staff other than the DSL must not view, copy, print, save, forward, ask for the image, ask a child to send it, or delete it.

They must not investigate the incident themselves. Staff record necessary non-image details and seek safeguarding advice about securing a device without accessing the material.

The DSL follows UKCIS Sharing nudes and semi-nudes advice, including the initial review, risk assessment, referral criteria, parental involvement and support. Images are not routinely viewed; any exceptional decision is made and recorded by the DSL under the guidance. AI-generated, altered and coerced images require the same safeguarding response. An apparent agreement to share does not remove concerns about coercion, exploitation or harm.

Staff respond supportively to all affected children. Threats to share images or demands for money or further images are urgent safeguarding concerns. Children should be helped to obtain appropriate reporting, removal and emotional support without reproducing the material.

Bullying harassment exploitation and extremism

Online bullying, harmful sexual behaviour, hate speech, covert recording and upskirting are handled under safeguarding and the relevant Behaviour and Anti-Bullying policies. Staff must not dismiss abuse as banter. The DSL considers the needs of victims, children displaying harmful behaviour and other affected pupils.

Concerns about grooming, exploitation or radicalisation are escalated promptly under safeguarding and Prevent procedures. Staff should consider threats, isolation, secrecy, coercive group activity and harmful contact through mainstream games, messaging and social platforms. An incident outside school still requires action where it affects a child's safety or wellbeing.

Harmful posts can be reported to the platform and specialist advice sought from the Professionals' Online Safety Helpline. Requests for removal must not compromise evidence or safeguarding advice. Staff must not circulate illegal material as evidence.

5 Filtering and monitoring

Filtering prevents access to harmful content; monitoring helps identify concerning activity. Both support safeguarding, alongside supervision, education and reporting. No system guarantees that all inappropriate material will be blocked or detected.

Governors have strategic oversight. Denis O'Regan, Emily Phipps and Jane McManus will oversee provision; the DSL leads its safeguarding use, and the IT provider maintains technical systems and supplies reports. Decisions about blocking, allowing access and exceptions will be documented with reasons

Provision must reflect primary-age pupils, SEND and other vulnerabilities, curriculum needs, school-managed devices on and off-site, mobile apps, and the limits of filtering dynamic or AI-generated content. Appropriate content should be blocked without unreasonable restrictions on learning. Any exception requires authorised, recorded risk assessment and review; staff must not bypass controls themselves.

The DSL, senior leaders and technical colleagues will review filtering and monitoring at least once every academic year with the responsible governor. Reviews record coverage, limitations, incidents, staff feedback, training needs and required actions. New devices, new platforms, significant software or configuration changes and emerging safeguarding risks trigger additional review and checks.

Regular operational filtering checks will be recorded separately from the annual review and from routine review of safeguarding reports. They must test relevant devices, networks, user groups and off-site arrangements.

Staff supervise pupil use and report access to unsuitable content, bypass attempts, excessive blocking and system failures to the DSL and IT provider. Where protection fails, staff stop or adapt the affected activity and leaders decide whether devices can safely remain in use pending repair.

The monitoring plan will identify who reviews alerts and filtering reports, how quickly different risks are escalated, backup cover, staff-related captures and out-of-hours arrangements. Urgent safeguarding alerts require prompt action. Access is limited to authorised staff, and incidents and outcomes are recorded securely.

Safe Search, video restrictions, approved search services and access to generative AI must be set and checked according to the risk assessment. Their limitations must be understood

6 Approved communication storage and learning platforms

School business involving pupils, families or school information must use approved, school-managed accounts and communication systems. Staff must not communicate privately with pupils through personal email, messaging accounts or social media. Pre-existing family connections must be declared and managed by the headteacher.

Messages must be professional, respectful and appropriate. The same expectations apply to email, learning platform comments, chats, blogs and shared documents. Pupils' communication permissions must be age-appropriate and supervised. Important safeguarding information must be passed through the safeguarding reporting route.

New apps or platforms, including free services and embedded chat or AI features, require approval before use. Leaders consult the DSL, IT provider and DPO about age restrictions, safeguarding, security, accessibility, personal data, contractual terms and monitoring. Accounts, sharing permissions and access must be centrally managed.

School data must be stored in approved locations with appropriate access, retention and secure sharing. Personal accounts and unofficial staff messaging groups must not be used to store or exchange confidential pupil or school information. Any mistaken use, accidental disclosure or loss must be reported immediately to the relevant headteacher, DSL and DPO through the incident procedure.

7 Generative AI

The Federation recognises potential educational benefits and risks from generative AI, including inaccurate outputs, bias, harmful advice, privacy loss, copyright concerns, impersonation and sexual image manipulation. Any use must have a clear educational or work purpose and remain under human responsibility.

Staff use only individually approved tools through authorised school accounts. Pupils must not independently access general-purpose AI services; any pupil-facing use requires specific approval, age-appropriate safeguards, close supervision and a documented educational rationale.

Before approving a tool, leaders consult the DSL, IT provider and DPO, assess age terms and the DfE product safety standards, consider a data protection impact assessment where required, and check how inputs, outputs, storage and model training are handled. Existing AI embedded in search, learning resources and administrative systems is included in the review.

Staff must not enter personal, sensitive or confidential information about children, families, staff or the school into generative AI tools. Any exceptional proposed use of personal data requires a separate lawful, approved process and DPO advice. AI must not replace professional safeguarding judgements, referrals or assessment of a child's needs.

Staff check generated resources and advice for accuracy, age suitability, bias, copyright and harmful content before use. They retain responsibility for planning and assessment. Pupils must not present AI-generated work as their own; any permitted assistance must be explained as required by the teacher.

AI notetakers, transcription bots and other automated recording tools must not be used in meetings or lessons without specific prior authorisation, a lawful basis, clear participant information and appropriate safeguarding and privacy controls.

Teaching and parent guidance will address misinformation, deepfakes, privacy, image manipulation and the risks of AI companions. Suspected misuse or harmful output is reported through safeguarding, data protection or staff conduct procedures as appropriate. Approved tools are reviewed when their functions or terms change.

8 Websites social media and digital images

Headteachers oversee school website and official social media content and ensure that only authorised staff publish material. Passwords, access permissions and account recovery arrangements must be managed securely

Publication must respect copyright, privacy and safeguarding. Public posts must not reveal confidential information, safeguarding status, children's contact details or unnecessary identifying details. Complaints about the school should use the school's complaints process; social media is not a suitable channel for confidential concerns about a child.

Staff must maintain professional boundaries and must not befriend, follow or privately message current pupils through personal accounts. Any exceptional pre-existing connection requires declaration and headteacher approval. Staff must not publish pupil images, confidential school information or unauthorised recordings through personal accounts. Families are asked to model respectful behaviour and use services in line with age restrictions and applicable law.

School photographs and recordings must have a defined purpose and lawful basis. Staff check current permissions and safeguarding restrictions before capture or publication, and respect withdrawal of consent where consent is the basis used. Public image use must be assessed for the risk of identification, copying and AI manipulation, even where permission exists.

Only school equipment is to be used for pupil images, avoid personal phones, minimise identifiable public images and avoid linking a child's full name with a photograph. Prefer non-identifying views where they meet the purpose. Any approved publication of identifiable imagery requires a recorded safeguarding assessment and appropriate permissions.

Images are transferred to approved storage, protected by access controls and retained or deleted according to the data protection schedule. Staff must prevent automatic upload to personal cloud accounts.

Parents and visitors must follow event-specific photography arrangements, must not covertly record people, and must not publish images of other children without appropriate permission. Authorised school publicity is separate from personal use. Pupils are taught to ask permission, avoid oversharing and report misuse of images.

9 Devices wearable technology and trips

Device rules apply to phones, smartwatches, smart glasses, cameras, microphones and any other connected or recording technology. Secret photography, audio or video recording, including remote activation, is prohibited. Personal recording devices require explicit written authorisation before use in school.

Personal phones and connected wearables are not used during the school day. Where permission to bring a device is granted, it is switched off and stored under the agreed school arrangements; parents use the school office for urgent contact.

Medical, disability and accessibility needs require an individual assessment with parents and relevant professionals, including necessary adjustments and arrangements for safe use. Restrictions must not prevent an agreed medical or accessibility function.

Staff keep personal phones silent and use them only in permitted staff areas away from pupils unless an authorised work or emergency need applies. Personal devices must not be used to download confidential school information or capture pupil images outside the approved arrangements. Volunteers, contractors, governors and visitors must follow the rules explained on arrival and obtain permission before any work-related photography.

Parents should keep phones away during interactions with staff or children, follow rules for school events and use the office for urgent pupil contact

School devices are used for approved purposes and software. Users must not disable security, install unauthorised software, share passwords or use VPNs, proxies or other methods to bypass safeguarding controls. Authorised technical tools require documented approval.

Off-site school devices remain subject to this policy. Leaders confirm filtering, monitoring, support and loss-reporting arrangements before issue. Staff must not encourage connection to an unassessed public or third-party network without considering the safeguarding and data security risks.

Trips must have an agreed communication plan, authorised equipment and emergency arrangements. Staff should use school duty phones or approved systems for contact with parents. Any emergency use of a personal phone must be reported promptly and handled to protect professional boundaries and confidential information.

Searching and confiscation are carried out only within lawful powers, by appropriately authorised staff and in accordance with DfE guidance and the Behaviour Policy. The presence of a device does not authorise an unrestricted search. Staff must follow the sexual imagery procedure and seek DSL or police advice where illegal material is suspected.

10 Data protection cyber security and review

Data protection and cyber security support safeguarding. Staff use strong unique passwords, multi-factor authentication where available or required, secure access, approved sharing and timely incident reporting. The IT provider maintains appropriate patching, malware protection, backup and recovery arrangements. Users report phishing, lost devices and suspected compromise promptly and do not continue using an unsafe system without advice.

Information is shared lawfully and proportionately to protect children. Data protection must not be used as a reason to withhold necessary safeguarding information. The DPO advises on privacy, access, retention and breaches; the DSL leads safeguarding decisions. Monitoring must be proportionate, access restricted and users appropriately informed.

The governing board receives proportionate assurance about incidents and trends, training, curriculum, filtering and monitoring review findings, and completion of actions, without unnecessary identifying information. Leaders evaluate how well children can recognise risk, seek help and receive support. Annual review includes consultation and changes to school practice, technology, safeguarding risks and guidance.

Appendix A Roles and responsibilities

Governing board

The board approves and monitors the policy, holds headteachers to account, assigns a responsible filtering and monitoring governor, and ensures suitable resources and training. It receives assurance about annual review, system checks, monitoring responses and educational provision, including adaptations for vulnerable pupils.

Headteachers and senior leaders

Leaders implement the policy, provide time and resources for DSLs and online safety leads, approve technology and risk assessments, oversee professional conduct and staff allegations, and ensure that linked policies and acceptable use agreements are consistent. They make sure approved arrangements are practicable and understood.

Designated Safeguarding Leads and deputies

DSLs retain lead responsibility for online safeguarding and the safeguarding use of filtering and monitoring. They respond to concerns, maintain records, coordinate referrals and support, work with IT colleagues and curriculum leads, analyse local trends and report assurance to leaders and governors. They ensure effective absence cover and clear escalation arrangements.

Online safety leads

Jamie Phillips at St John's and Justina Oduko at St James the Great support coordination, training, parent engagement, curriculum development, Safer Internet Day activity, incident trend review and policy updates. They work with the DSL and must not become a substitute reporting route that delays safeguarding action.

All staff including supply staff

Staff read and follow this policy, the Staff Code of Conduct, applicable KCSIE information and acceptable use agreement. They model safe behaviour, supervise pupil technology use, teach relevant safety skills, protect school data, attend training and promptly report safeguarding concerns and technical weaknesses. They understand their own filtering and monitoring responsibilities.

Curriculum leads and subject leaders

Computing and PSHE or RSHE leads coordinate a progressive, complementary curriculum, assessment and adaptations, working with DSLs and online safety leads. Other subject leaders embed relevant teaching and safe use of technology. Staff use local evidence to inform lessons and avoid gaps or conflicting messages.

IT provider and technical staff

Technical staff maintain secure systems, implement agreed filtering and monitoring, document settings and limitations, provide reports and support regular checks and annual reviews. They test new devices and services before release, escalate safeguarding concerns to the DSL, remedy faults and support incident response without independently deciding safeguarding outcomes.

Data Protection Officer

The DPO advises on lawful processing, privacy notices, impact assessments, retention, sharing, contracts, access controls and breaches. Advice supports necessary safeguarding information sharing and proportionate use of monitoring, images, AI and recording systems.

Pupils

Pupils learn and follow age-appropriate acceptable use rules, respect others, protect personal information, use approved services and tell a trusted adult about worrying content or contact. Pupils must be supported to report mistakes and harm without fear of blame.

Parents and carers

Families support safe behaviour, talk to children about online activity, follow school communication and image rules, respect applicable age restrictions and inform the school of concerns. They seek urgent statutory help where needed rather than relying on unattended school messages.

Volunteers contractors and external groups

These users receive and follow applicable acceptable use rules, maintain professional boundaries, avoid unauthorised recording and report concerns promptly. External tutors must not arrange private pupil contact or meetings outside school-authorised arrangements. Groups hiring premises must follow the technology and safeguarding conditions of use.

Appendix B Guidance and national context

This draft uses the supplied July 2026 LGfL template and the existing Federation policy as its principal sources. National themes reflected in the draft include AI-generated harmful content, manipulation of images, coercive contact and extortion, harmful online groups, discriminatory behaviour, misinformation and cyber attacks. These are risk areas for consideration, not assertions that incidents have occurred at either school. The template's statistical national landscape appendix has not been reproduced; local audit evidence should guide priorities.

The following official guidance should be used in its current applicable version. Selected official sources were checked during preparation on 9 October 2026; the list also provides related guidance for the final school review. Before approval, leaders should check updates, legal commencement and any Southwark-specific requirements.

- Keeping children safe in education https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Teaching online safety in schools https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- DfE filtering and monitoring core standard https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard
- Generative AI in education https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education
- Generative AI product safety standards https://www.gov.uk/government/publications/generative-ai-product-safety-standards
- Sharing nudes and semi-nudes https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- Searching screening and confiscation https://www.gov.uk/government/publications/searching-screening-and-confiscation
- Relationships education relationships and sex education and health education https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education