ST JAMES INFANT & PRE-SCHOOL
Online Safety Policy
2026–2027

Policy status	School safeguarding policy supporting statutory duties
Policy lead	Headteacher and Designated Safeguarding Lead
Technical lead	Trust / school IT support provider
Named governor	To be confirmed by the Local Governing Body
Date approved	To be completed following approval
Review date	September 2027, or sooner if required

Our commitment: At St James, children learn to enjoy technology safely, kindly and confidently. Adults provide close supervision, effective technical protection and calm, child-centred support so that every child knows: Stop, close it, tell a trusted adult.

This policy should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour and Relationships Policy, Staff Code of Conduct, Acceptable Use Agreements, Data Protection Policy, Mobile Phone and Camera arrangements, Prevent risk assessment, curriculum policies, complaints procedure and incident-response arrangements.

1. Purpose and principles

This policy explains how St James Infant & Pre-School safeguards children, staff and the wider community when technology is used in school, at home for school purposes, or in a way that affects school life. Online safety is a safeguarding responsibility and an essential part of learning, relationships, behaviour, data protection and digital leadership. It is not limited to computing lessons or school-owned devices.

The school will provide an age-appropriate online safety curriculum, safe systems and effective adult supervision. Children will be listened to, believed and supported without blame. Staff will remain professionally curious because online harm can occur on any connected device and can affect very young children through videos, games, messaging, live streaming, advertising, connected toys, voice assistants, artificial intelligence and the online activity of other people around them.

2. Scope and the four areas of online risk

This policy applies to pupils from Preschool to Year 2, staff, governors, volunteers, contractors, visitors, parents and carers where they use school systems or their online activity affects a child or the school. It covers school networks and accounts, school and personal devices, cloud services, educational applications, social media, messaging, gaming, cameras, smart devices, wearable technology and artificial intelligence.

The school considers the four interrelated areas of risk identified in statutory safeguarding guidance: content, contact, conduct and commerce. Content includes illegal, inappropriate, misleading or harmful material. Contact includes harmful interaction, grooming, coercion, exploitation and unwanted communication. Conduct includes bullying, unsafe sharing, impersonation and behaviour that harms self or others. Commerce includes scams, gambling-like features, phishing, advertising, in-app purchases and other financial exploitation. Risks may involve child-on-child abuse, adults, automated systems or AI-generated material and may cross the boundary between home and school.

3. Legal and guidance framework

The school will have regard to Keeping Children Safe in Education 2026 from 1 September 2026, including its requirements for a whole-school approach to online safety, appropriate filtering and monitoring, staff awareness and the DSL's lead responsibility. The policy also reflects the Education Act 2002, Children Acts 1989 and 2004, Counter-Terrorism and Security Act 2015, Equality Act 2010, Human Rights Act 1998, UK GDPR and Data Protection Act 2018, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and relevant criminal law.

For Preschool and Reception, the school will meet the safeguarding and welfare requirements of the Early Years Foundation Stage statutory framework in force from September 2026, including clear arrangements for mobile phones, cameras and devices with imaging or sharing capability. Curriculum provision will reflect the National Curriculum for computing and statutory Relationships and Health Education guidance introduced from September 2026.

4. Leadership, governance and accountability

The Trust and Local Governing Body

The Trust and Local Governing Body will ensure that online safety is a running and interrelated theme in safeguarding, curriculum, behaviour, staff development, procurement and risk management. They will ensure appropriate filtering and monitoring are in place, review the DfE standards, assign responsibilities, receive assurance about effectiveness and challenge leaders about risks, incidents, training and vulnerable pupils. Governors will complete relevant safeguarding and filtering-and-monitoring training and comply with the staff and governor Acceptable Use Agreement.

The Headteacher

The Headteacher is accountable for implementation, culture and resources. They will ensure that staff understand the policy, approved systems are used consistently, concerns are acted on promptly, technical and safeguarding teams cooperate, and children and parents receive appropriate education. The Headteacher will ensure that new technology, services and AI tools are risk assessed before use and that contracts provide suitable security, privacy, accessibility, filtering and incident support.

The Designated Safeguarding Lead

The DSL has lead responsibility for online safety and for understanding the filtering and monitoring systems and processes used by the school. The DSL will coordinate safeguarding responses; receive and analyse relevant alerts and incident information; ensure that risks are reflected in the safeguarding curriculum and staff training; support children and families; liaise with IT support, the DPO, social care, Prevent partners and police where necessary; and report themes and assurance to the Headteacher and governors without identifying children unnecessarily.

Technical and data-protection leads

The Trust or school IT support provider will implement and maintain approved security, filtering and monitoring controls; ensure coverage across networks, users and school-managed devices; manage accounts, permissions, updates, backups and logs; test systems; respond promptly to faults and alerts; and explain the operation and limitations of systems to the DSL and leaders. The Data Protection Officer will advise on lawful, fair and transparent processing, data-protection impact assessments, breaches, contracts and high-risk technologies.

All staff and volunteers

All staff and volunteers must model safe and professional behaviour, use only authorised accounts and services, supervise pupils actively, teach and reinforce child-friendly safety routines, maintain confidentiality, respond calmly to disclosures, and report concerns through the safeguarding system. They must report any filtering or monitoring concern or failure immediately to the DSL and IT support and must never disable or bypass controls without documented authorisation for a legitimate purpose.

5. An infant-school approach to online safety education

Children will be taught through short, frequent, concrete and revisited learning rather than being given responsibility they are too young to carry. Teaching will use stories, puppets, role play, photographs, visual prompts, modelling and supported practice. The consistent child-facing message is: Stop; close or turn the screen away; do not reply or share; tell a trusted adult; keep telling until someone helps. Children will learn that they will not be in trouble for asking for help and that harm is never the child's fault.

From Preschool, children learn that devices belong to people, adults help us use them, some things are private, photographs need permission and uncomfortable content should be shown to a trusted adult. In Reception, children practise choosing trusted adults, asking before clicking or taking a photograph, using kind words, recognising adverts and keeping names, addresses and passwords private. In Years 1 and 2, children develop these concepts through safe and respectful use, simple password security, reliable information, ownership of digital work, online friendships, reporting, scams, persuasive design and the effects of sharing. Teaching will be honest but will not introduce frightening or developmentally inappropriate detail.

Online safety will be taught through computing, Relationships and Health Education, Protective Behaviours, assemblies, stories and teachable moments. The curriculum will address the school's contextual risks and will be updated when patterns change. It will explicitly teach consent and boundaries for photographs and communication, respectful behaviour, the difference between a surprise and an unsafe secret, and that a person online may not be who they claim to be.

6. Inclusion, SEND, EAL and vulnerability

Teaching and protection will be adapted because a single approach will not meet every child's needs. Children with SEND, communication differences, developmental delay, sensory needs, social understanding difficulties, trauma, care experience or limited English may be more vulnerable to manipulation, literal interpretation, repeated exposure or difficulty reporting. Children may also have greater reliance on technology for communication and access, which must not be unnecessarily restricted.

Adaptations may include Widgit symbols, now-and-next boards, social stories, concrete examples, repetition, reduced language, supported choice, pre-teaching, personalised safety plans, additional supervision and trusted-adult check-ins. Staff will listen to behaviour and non-verbal communication as

possible indicators of concern and will avoid assuming that a child understands a safety rule because they can repeat it.

7. Filtering and monitoring

The school will use filtering and monitoring that is appropriate to the age and risk profile of its pupils, the number and type of devices, SEND and accessibility needs, curriculum requirements, remote and cloud use, and the risk presented by real-time, dynamic, personalised and AI-generated content. Filtering will block harmful and inappropriate content, including illegal content and terrorist material, without unreasonably restricting teaching and learning. Monitoring will enable the school to identify concerning activity and respond proportionately.

Roles will be documented across governance, senior leadership, the DSL and technical support. Provision will be formally reviewed at least once every academic year and sooner following a safeguarding incident, significant system change or identified weakness. The review will include checks that filtering works on all relevant networks and devices, monitoring reports are reaching the right people, concerns are acted on, user groups and exceptions are appropriate, and pupil risk profiles and emerging technologies are considered. Outcomes and actions will be recorded and reported to governors.

Filtering and monitoring support, but do not replace, supervision, education and professional judgement. Staff must not assume that a filtered device is risk free. Approved blocking tests will be conducted safely by authorised adults; staff must not search for illegal material to test the system. A request to unblock content will be educationally justified, risk assessed, authorised and logged. Safeguarding overrides will be tightly controlled, time limited and auditable.

8. Supervision and acceptable use by pupils

Pupils will use school technology only with adult knowledge and appropriate supervision. Staff will select content in advance where practicable, use child-safe settings and accounts, position screens so use can be supported, and intervene promptly if unexpected content appears. Children will not independently create public accounts, communicate with unknown people, make purchases, livestream, publish personal information or install applications through school activity.

Acceptable use will be explained in developmentally appropriate language and revisited regularly. Where a child makes an unsafe choice, adults will first secure safety and understand what happened. Responses will be proportionate, educational and consistent with the Behaviour and Relationships Policy; support and reasonable adjustments will be considered before sanctions. Access will not be removed in a way that prevents a child receiving education or a necessary communication adjustment unless there is an immediate safety reason and an alternative is provided.

9. Personal devices, mobile phones, cameras and smart technology

Pupils must not use mobile phones, smart watches or other personal connected devices during the school day. Any device brought for an agreed exceptional reason must be switched off and stored as directed. Individual arrangements may be made for a medical, disability or safeguarding need following risk assessment. Parents must not photograph or record children on site or at events except where the school has expressly permitted this and made the boundaries clear.

Staff and visitors will follow the school's mobile phone and camera arrangements, with particularly strict controls in Preschool and Reception. Personal devices must not be used to photograph, film or record pupils, access pupil records, or communicate privately with pupils. Images and recordings for school

purposes will be made only on authorised equipment or systems, for an identified purpose, with appropriate transparency and consent arrangements, and will be stored, shared and deleted securely.

10. Accounts, passwords and access

Each authorised user will use their own account and keep credentials confidential. Staff must use multi-factor authentication where provided, approved password practices and screen locking, and must not allow pupils to use an adult account. Access will follow least-privilege principles and will be removed or amended promptly when roles change or people leave. Shared pupil accounts, where developmentally necessary, will be limited and risk controlled.

Suspected compromise, unexpected authentication requests, phishing, lost devices or accidental disclosure must be reported immediately. Users must not attempt to investigate a cyber incident themselves, connect unknown storage devices, install unapproved software or forward suspicious content. Technical staff will preserve relevant logs and follow the Trust's cyber-incident and data-breach procedures.

11. Staff professional conduct and communication

Staff must maintain professional boundaries online and comply with the Staff Code of Conduct. Communication with parents will take place through approved school channels such as school email, telephone and ClassDojo. Staff must not accept or initiate contact with pupils through personal social-media, gaming or messaging accounts, and must not use personal accounts to discuss identifiable school matters. Privacy settings do not remove professional responsibilities.

Online content created or shared by staff must not bring the school or profession into disrepute, disclose confidential information, undermine safeguarding or compromise public confidence. Any allegation or low-level concern involving an adult's online conduct will be managed under the safeguarding, low-level concerns and allegations procedures, including referral to the LADO or other agencies where required.

12. Generative artificial intelligence

AI tools may create inaccurate, biased, manipulative, age-inappropriate or convincing harmful material and may process prompts and uploads in ways that are not immediately visible. Pupils in Preschool to Year 2 will not independently access open-ended generative AI services through school. Any pupil-facing AI activity must use an approved, age-appropriate product, have a clear educational purpose, be risk assessed and closely supervised, with outputs checked by a competent adult before children see or use them.

Staff may use only approved AI tools and must follow the school's AI, data-protection, copyright and procurement requirements. Personal, special-category, safeguarding or confidential information must not be entered into a public AI service. Staff will apply the DfE's safe-use principles, fact-check outputs, check bias and accessibility, preserve professional judgement, acknowledge material use where appropriate, and never use AI as the sole basis for a safeguarding, assessment, disciplinary or high-impact decision. A data-protection impact assessment will be considered before introducing high-risk processing.

AI-generated impersonation, sexualised imagery, manipulated photographs, bullying, fraud or harmful misinformation will be treated according to the nature and impact of the conduct, not dismissed because it is synthetic. Leaders will consider safeguarding, criminal, data-protection and reputational implications and will preserve evidence without circulating harmful content.

13. Online bullying and child-on-child abuse

Online bullying may include repeated or one-off harmful messages, exclusion, humiliation, impersonation, image sharing or behaviour that continues beyond the school day. A single incident can have a serious or lasting effect and may constitute child-on-child abuse even when it does not meet the school's definition of bullying. The school will respond to harmful online behaviour that affects pupils' safety, welfare, relationships or learning, whether it began on or off site.

Staff will record the child's account in their own words, reassure them, avoid blame, assess immediate risk, inform the DSL and preserve available evidence. The school will support the child harmed and respond to the child who caused harm in a developmentally informed way. Parents will normally be involved unless doing so would increase risk. Repeated, sexual, discriminatory, threatening or criminal behaviour will be escalated under safeguarding procedures.

14. Sexual content, grooming and harmful contact

Very young children may encounter sexual content accidentally, be coerced into producing or viewing an image, or be affected by an adult's device or behaviour. Any sexualised online incident involving a child will be treated as a safeguarding concern. Staff will not ask a child to show, forward, download or delete a nude or sexual image, and will not view such content unless this is unavoidable and necessary to safeguard the child under the direction of the DSL and relevant national guidance.

The device should be secured without searching it, evidence preserved and the DSL informed immediately. The DSL will follow current UKCIS and KCSIE guidance, consider social care and police involvement, record decisions and protect the child from further sharing or shame. Staff will not promise confidentiality. Teaching will remain age appropriate and will emphasise body privacy, permission, trusted adults and that children are never responsible for abuse.

15. Radicalisation, extremism and hateful content

The school will protect children from online radicalisation and extremist or hateful content through the Prevent duty, appropriate filtering, staff vigilance, an inclusive curriculum and timely safeguarding action. At infant age, concerns may arise from language, symbols, videos, games, family or peer influence, repeated themes in play, or material encountered on a device. Staff will record context carefully and refer concerns to the DSL rather than attempting to test a child's beliefs or investigate independently.

The DSL will assess the concern using the school's Prevent procedures and local arrangements, seek advice where required and make a referral when the threshold is met. Legitimate discussion, faith, culture and protected beliefs will be respected; action will be based on safeguarding risk, not stereotype.

16. Misinformation, advertising, scams and commercial pressure

Children will learn that online material can be designed to persuade, collect information or make people spend money. Teaching will help them recognise adverts, in-app purchases, reward loops, false claims and unfamiliar links, and practise asking an adult before clicking, downloading or buying. Staff will choose resources that minimise advertising, tracking and commercial influence and will not encourage pupils to provide personal data in exchange for access or rewards.

Phishing, fraud, suspicious payment requests and account compromise must be reported immediately through the school's cyber-security arrangements. Staff will verify unusual requests using a separate trusted contact method and will never ask pupils to deal with financial or account-security messages.

18. Responding to a concern or incident

The immediate priorities are the child's safety, preservation of evidence and prevention of further harm. A member of staff receiving a concern will listen calmly, use open and minimal questions, avoid investigating, explain that the information must be shared with the DSL, record the child's words and context, and report without delay. If there is immediate danger, staff will call 999 and then follow safeguarding procedures.

The DSL will assess content, contact, conduct and commerce risks; identify all children involved; consider vulnerability, SEND, coercion and power imbalance; decide on parental involvement; and consider referrals to children's social care, police, Prevent, CEOP or other services. Illegal or suspected illegal material will not be copied, printed, forwarded or unnecessarily viewed. Technical logs and devices will be preserved where appropriate, and any data breach will be referred promptly to the DPO. Decisions, rationale, actions and review will be recorded on the school's safeguarding system.

Filtering alerts are indicators, not proof of wrongdoing. They will be reviewed in context by authorised staff, with access limited to those who need the information. The school will avoid blanket surveillance, excessive collection or automated decisions without human review. Children and staff affected by an incident will receive proportionate support, and lessons for curriculum, supervision or systems will be implemented.

20. Data protection, images and educational technology

Personal data will be processed lawfully, fairly, transparently and securely. The school will minimise data, use approved storage and sharing methods, follow retention schedules and respond to breaches. Privacy information will explain relevant uses of technology. Children's work, image or voice will not be published or shared beyond the intended audience without an appropriate lawful basis and safeguards; consent will be freely given where consent is relied upon and can be withdrawn.

Before procuring or adopting an application, platform, connected toy or AI service, leaders will consider educational need, age suitability, account model, advertising, tracking, profiling, security, international transfers, retention, accessibility, supplier terms, parental information, filtering compatibility and deletion or exit arrangements. Free access does not remove these duties. Unapproved applications and personal cloud storage must not be used for pupil information.

21. Cyber security and continuity

Online safety depends on resilient and secure technology. The school and Trust will work towards and review the DfE cyber-security standards, including governance, asset management, supported software, secure configuration, multi-factor authentication, backups, incident response, staff awareness and supplier management. Security updates will be applied promptly according to risk, and backups will be protected and tested.

A suspected cyber incident will be reported immediately to IT support and the Headteacher. Users will follow instructions, which may include disconnecting a device without switching it off, changing credentials from a safe device or stopping use of a service. The school will activate its cyber-incident, business-continuity, safeguarding and data-breach arrangements and notify external bodies where required.

22. Training and awareness

All staff will receive online-safety and filtering-and-monitoring information at induction, safeguarding training at least annually, and updates when risks, systems or guidance change. Training will include infant-specific indicators, disclosures, harmful sexual content, child-on-child abuse, Prevent, AI, data protection, cyber security, professional boundaries, incident reporting and the operation and limitations of technical controls. The DSL and deputies will maintain knowledge through role-appropriate updates, and technical staff will receive training suitable to their responsibilities.

Governors will receive enough training to provide effective challenge. Pupils will receive continuous curriculum teaching, and parents will be offered accessible information. Leaders will evaluate whether training changes knowledge and practice rather than recording attendance alone.

23. Monitoring, evaluation and review

The DSL and Headteacher will review safeguarding records, filtering and monitoring information, cyber incidents, behaviour patterns, curriculum coverage, pupil voice, parent feedback, complaints and the experience of vulnerable groups. Information will be used to identify patterns and improve teaching, supervision, systems and support. Reports to governors will be anonymised and proportionate.

This policy and the school's online-safety risk assessment will be reviewed at least annually and sooner following a serious incident, significant system or legal change, an identified control failure or a change in the school's contextual risks. The filtering and monitoring effectiveness review will be recorded separately and reported through governance arrangements.

Key legislation and guidance

This policy has been written with regard to the following legislation, statutory guidance and national standards. The current version will be used where guidance changes during the policy period.

- DfE: Keeping Children Safe in Education 2026 (effective 1 September 2026)
- DfE: Filtering and monitoring core standard; Cyber security core standard; Digital leadership and governance standards
- DfE: Relationships Education, Relationships and Sex Education and Health Education guidance (for introduction 1 September 2026)
- DfE: Teaching online safety in schools; National Curriculum computing programmes of study
- DfE: Early Years Foundation Stage statutory framework for group and school-based providers (September 2026)
- DfE: Data protection in schools; Generative AI and data protection in schools
- DfE: Generative artificial intelligence in education and Generative AI product safety standards
- DfE: Searching, screening and confiscation; Behaviour in schools
- Home Office: Prevent duty guidance for England and Wales
- UKCIS: Sharing nudes and semi-nudes – advice for education settings
- UKCIS: Education for a Connected World and early-years online-safety guidance
- Data Protection Act 2018 and UK General Data Protection Regulation

Related school and Trust policies

This policy should be implemented alongside the Child Protection and Safeguarding Policy; Behaviour and Relationships Policy; Staff Code of Conduct; Acceptable Use Agreements; Data Protection Policy and

privacy notices; Mobile Phone and Camera Policy; Prevent risk assessment; Computing, Relationships and Health Education and PSHE policies; Anti-Bullying Policy; Complaints Procedure; Educational Visits Policy; Remote-Working arrangements; Cyber-Incident and Business-Continuity Plans; and disciplinary, whistleblowing and low-level-concerns procedures.