St Joseph's Catholic Primary Academy

Love, Learn and Live in Christ

Online Safety Policy

2025/2026

Review Date	Changes Made	Amended By
September 2027		Mrs S Stewart

Mission Statement

St Joseph's is committed to protecting pupils, staff, volunteers, governors and visitors from harm when using digital technology. We aim to provide a safe and secure environment, promote responsible online behaviour and help children develop the knowledge and confidence to use technology safely, respectfully and thoughtfully.

Our Catholic ethos is at the heart of this commitment and we believe that each person is a unique gift of a loving God. We seek to create an environment of trust, respect, tolerance, honesty and forgiveness, where every member of St Joseph's family is valued and treated with dignity.

Online safety is part of safeguarding and is the responsibility of everyone. It applies to the use of school equipment and networks, personal devices used on school premises, and online behaviour outside school where this affects the welfare of pupils or the school community.

1. Aims

St Joseph's aims to:

- have robust arrangements to safeguard pupils, staff, volunteers and governors when using technology;
- identify and support pupils who may be at greater risk of harm online, including pupils whose age, additional needs, communication needs or circumstances may increase their vulnerability;
- provide age-appropriate teaching that enables pupils to recognise risks, make safer choices and seek help;
- ensure staff understand their responsibilities for supervision, filtering, monitoring and reporting concerns;
- maintain effective filtering and monitoring arrangements and review them regularly;
- respond promptly, proportionately and consistently to online safety incidents; and
- work in partnership with parents and carers to promote safe and responsible use of technology.

2. Online safety risks – the four categories

Our approach considers the four categories of online risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, including pornography, racist or misogynistic material, antisemitism, extremist or terrorist content, content promoting self-harm or suicide, misinformation, disinformation and conspiracy theories.
- **Contact:** being subjected to harmful interaction with other users, including peer pressure, cyberbullying, grooming, adults pretending to be children, exploitation, commercial advertising and unwanted or harmful interactions with generative AI applications.
- **Conduct:** personal online behaviour that causes or increases the likelihood of harm, including bullying, harassment, sharing personal information, creating or sharing explicit images, non-consensual sharing of nude or semi-nude images, and the creation or sharing of AI-generated explicit or manipulated images (deepfakes).
- **Commerce:** risks such as phishing, scams, inappropriate advertising, financial exploitation and exposure to gambling-related content.

These categories overlap. The school recognises that online harm may occur through websites, search engines, social media, messaging services, games, livestreaming, apps, connected devices and AI tools. The school will keep its approach under review as technology and risks change.

3. Legislation and guidance

This policy should be read alongside the school's safeguarding and related policies. It is informed by the current versions of:

- Keeping Children Safe in Education 2026 (KCSIE), including Part One and the online safety and filtering and monitoring sections;
- Working Together to Safeguard Children;
- the Department for Education's Teaching Online Safety in Schools guidance;
- the DfE Meeting Digital and Technology Standards in Schools and Colleges, including Filtering and Monitoring: Core Standard;
- UK Council for Internet Safety (UKCIS) Education for a Connected World;
- the DfE guidance on searching, screening and confiscation and UKCIS guidance on sharing nudes and semi-nudes;
- the Data Protection Act 2018 and UK GDPR; and
- the National Curriculum computing programmes of study and statutory Relationships Education and Health Education requirements.

4. Roles and responsibilities

Academy Council / governing body

The Academy Council / governing body has strategic oversight of online safety and will hold the Headteacher to account for implementation. It will:

- ensure appropriate filtering and monitoring systems are in place and that provision is reviewed at least annually;
- ensure the annual review involves the senior leadership team (SLT), DSL, IT support and the governor responsible for safeguarding / online safety;
- receive appropriate assurance and reports about online safety, filtering and monitoring, incidents, actions and outcomes;
- ensure online safety is included in the school's safeguarding arrangements and that pupils are taught how to keep themselves and others safe online; and
- support appropriate training for governors.

Safeguarding governor: Mrs Joanna Grogan

Headteacher

- ensures this policy is understood and implemented consistently;
- ensures staff receive safeguarding and online safety training at induction and regular updates, at least annually;
- ensures staff understand the school's filtering and monitoring arrangements, how alerts are escalated and how concerns are recorded;
- promotes a culture in which pupils can report concerns without fear of blame;
- ensures filtering and monitoring systems are implemented, maintained and reviewed with the DSL and IT support; and
- ensures any temporary exception to filtering or monitoring is authorised, risk assessed and recorded.

Smoothwall currently provides the school's filtering and monitoring service. The school's stated arrangements include alerts to relevant senior leaders, the DSL, the caretaker and IT technician, with urgent/high-risk alerts also notified by telephone, and weekly reporting to the Headteacher. These arrangements must be checked with the

provider and kept under review. Receipt of a weekly report must not be treated, by itself, as proof that no safeguarding concern or breach has occurred.

Designated Safeguarding Lead (DSL) and deputies

The DSL has lead responsibility for online safety as part of the school's safeguarding arrangements. The DSL will:

- understand the filtering and monitoring systems and lead the safeguarding response to concerns identified through them;
- review relevant alerts and reports, decide what safeguarding action is required and ensure concerns are escalated promptly;
- ensure incidents, decisions, actions and outcomes are recorded on CPOMS in line with the Child Protection and Safeguarding Policy;
- liaise with the Headteacher, IT support, parents/carers and external agencies as appropriate;
- ensure online child-on-child abuse, cyberbullying and concerns involving AI-generated or manipulated images are treated as potential safeguarding matters and not simply as behaviour issues;
- contribute to the annual filtering and monitoring review and provide safeguarding assurance to the governing body; and
- ensure staff training and pupil education reflect current risks.

The DSL and deputy DSL details are set out in the Child Protection and Safeguarding Policy.

IT technician / IT support provider

IT support has technical responsibility for maintaining filtering and monitoring systems, providing reports and completing technical actions. Working with the Headteacher, DSL and relevant governor, IT support will:

- maintain Smoothwall and related systems and ensure they are configured appropriately;
- check that filtering and monitoring apply to all relevant school-managed internet-connected devices, services, user groups and locations, including devices used off-site where applicable;
- ensure student, staff and guest access profiles are appropriately configured;
- support the school's annual review, identify technical limitations and advise on mitigation;
- ensure safe search is enabled and locked where technically possible, and advise on controls that prevent circumvention of filtering;
- test filtering and monitoring on new devices, services and significant system changes before they are made available;
- provide weekly monitoring reports and immediate alerts for high-risk concerns in accordance with the agreed service configuration;
- keep a record of technical checks, issues, actions and outcomes, and report failures or gaps promptly; and
- maintain appropriate cyber security, malware protection, updates and access controls.

Computing coordinator

- ensures online safety is planned and taught through the curriculum and wider school activities;
- supports age-appropriate pupil understanding of online risks, including AI and manipulated content;

- ensures pupils are reminded of and agree to the relevant pupil acceptable use agreement at the start of each academic year;
- reports incidents and concerns to the DSL and records them in accordance with school procedures; and
- keeps their knowledge of online safety developments and relevant training up to date.

All staff, supply staff, contractors and volunteers

- read and follow this policy, the Child Protection and Safeguarding Policy, the Staff Code of Conduct and the relevant acceptable use agreement;
- supervise pupils when they use devices and carry out appropriate in-person monitoring, including being alert to what pupils are viewing and doing;
- know how to report concerns, filtering alerts, unsuitable material, technical failures or attempts to bypass controls;
- report concerns to the DSL or deputy without delay and record them on CPOMS in line with school procedures;
- never use personal accounts or personal messaging services to communicate with pupils;
- use digital communication with pupils only through authorised school systems and for legitimate professional purposes;
- protect personal and sensitive school information and follow data protection requirements;
- maintain professional conduct when using technology, including outside school where conduct may affect their suitability to work with children; and
- embed online safety messages in learning where appropriate.

Parents and carers

- support the school's approach to online safety and reinforce safe, respectful use of technology at home;
- take an interest in children's online activities, including games, apps, websites and who they communicate with;
- raise concerns with the Headteacher or DSL; and
- engage with information and guidance shared by the school.

Pupils

- follow the pupil acceptable use policy and school rules for devices and the internet;
- treat others respectfully online and protect their own and other people's personal information;
- tell a trusted adult if something online makes them worried, uncomfortable or unsafe, or if they see something harmful happening to someone else;
- not create, request, save, forward or share harmful or inappropriate content, including manipulated or AI-generated images of others; and
- follow school policies on online bullying and responsible use of technology.

Visitors

Visitors and members of the community using school devices or the school network will be made aware of the relevant acceptable use requirements and must follow them.

5. Teaching pupils about online safety

Online safety is taught as part of a broad and balanced curriculum, including Computing, Relationships Education, Health Education and PSHE. Teaching will be progressive, age-appropriate and revisited regularly. It will reflect the pupils' developmental stage, communication needs and individual vulnerabilities.

Pupils will be taught to:

- keep personal information private and understand how information and data are collected, shared and used online;
- recognise that people may behave differently online or pretend to be someone they are not;
- understand that online relationships should be respectful and that the same expectations of kindness and respect apply online and offline;
- recognise inappropriate content, contact and conduct, including grooming, bullying, pressure, scams and harmful challenges;
- think critically about online information, including misinformation, disinformation, advertising and AI-generated content;
- understand that images, audio and video can be edited or generated and may not be genuine;
- understand safe boundaries and how to respond to unwanted contact or requests for personal information or images;
- manage screen time and consider the impact of online experiences on wellbeing;
- know how to block, report and seek help, and understand that they will be listened to if they raise a concern; and
- understand that sharing, forwarding or commenting on harmful content can increase the harm caused.

Where appropriate, teaching and resources will be adapted for pupils with SEND, pupils with communication needs and pupils who may need additional support to understand online relationships, boundaries or risk.

6. Partnership with parents and carers

The school will raise parents' and carers' awareness of online safety through letters, the school website, ClassDojo, information sessions and other appropriate communications. The school will share this policy and provide information about:

- the filtering and monitoring systems used by the school and the broad nature of how they operate;
- the types of online activities pupils may be asked to undertake and the platforms or services used for learning;
- current risks and practical ways to support children's online safety at home; and
- how parents and carers can report concerns to the school.

Parents and carers should raise concerns in the first instance with the Headteacher or DSL. The school will signpost families to reputable online safety advice where appropriate.

7. Filtering and monitoring

The school uses Smoothwall for filtering and monitoring. Filtering is intended to prevent access to illegal, inappropriate or harmful content. Monitoring is intended to identify activity that may indicate a safeguarding or technical concern. Neither system is a substitute for active supervision, good teaching or prompt safeguarding action, and no filtering system can guarantee that all harmful content will be blocked.

Responsibilities and review

The governing body has strategic responsibility for ensuring appropriate systems are in place. The annual review will be led by the SLT and DSL, with IT support and the safeguarding governor involved. The review will be recorded, including findings, decisions, actions, owners and completion dates.

The review will consider at least:

- pupils' age, needs, SEND, communication needs, EAL and safeguarding risk profile;
- what the filtering system blocks and allows and any technical limitations;
- all school-managed devices and services, including devices used off-site, and all relevant premises and network connections;
- student, staff and guest profiles and any bring-your-own-device arrangements;
- use of apps, mobile technologies, browsers, search engines and generative AI tools;
- monitoring alerts, reports, safeguarding incidents, near misses and actions taken;
- the effectiveness and frequency of manual and technical monitoring;
- whether safe search is enabled and whether controls to prevent circumvention are effective;
- staff awareness, training, reporting routes and curriculum coverage; and
- whether changes to technology, software, network configuration or working practices require an earlier review.

A further review will take place when a significant safeguarding risk is identified, new technology or AI tools are introduced, devices or services change, major software or network changes occur, or working practices change in a way that may affect filtering or monitoring.

Checks and records

The school will undertake and record checks at a frequency informed by the annual review and risk assessment. Checks must establish that systems remain active and correctly configured, have not been disabled or bypassed, and cover relevant devices, services, user groups and locations. Records will include the date, person completing the check, what was tested, the outcome and any action taken.

The monitoring plan will include at least weekly reports highlighting incidents and immediate reporting of high-risk alerts, in line with the DfE core standard and the school's Smoothwall configuration. The school will make sure reports are reviewed by an appropriate person, concerns are referred to the DSL promptly and outcomes are recorded.

Any temporary exception to filtering or monitoring must be approved in advance by the SLT member responsible for the system, with the DSL considering safeguarding implications. The reason, scope, duration, authorisation and safeguards must be documented. Exceptions must be removed when no longer required.

Staff must report immediately if they encounter unsuitable material, suspect a pupil has accessed or created it, identify a system failure or possible circumvention, or believe filtering is unreasonably preventing legitimate learning.

8. Use of devices, the internet and AI

School internet and devices

School internet and devices are provided to support teaching, learning, communication and the professional work of staff. Users must follow the relevant acceptable use agreement. Users should understand that activity on school systems and devices may be filtered or monitored for safeguarding, security and operational purposes. The school will make users aware of monitoring arrangements and handle monitoring information in accordance with data protection requirements.

Artificial intelligence (AI)

The school recognises that AI tools may support learning and professional work but may also create safeguarding, privacy, accuracy and integrity risks. Any AI product or feature used with pupils or staff for school purposes must

be approved through the school / Trust's process and assessed for safeguarding, age suitability, data protection, security and educational value before use.

Pupils will receive age-appropriate teaching about AI, including that AI-generated information can be inaccurate, biased or misleading; that images, audio and video can be generated or manipulated; and that personal information, photographs or identifiable details must not be entered into unauthorised tools. Pupils must report AI interactions or generated content that make them feel unsafe or uncomfortable.

The creation, use or sharing of AI-generated or manipulated content to bully, threaten, humiliate, exploit or sexualise a pupil will be treated as a serious safeguarding concern and managed under the Child Protection and Safeguarding Policy and, where appropriate, the Behaviour Policy. Staff must not upload identifiable pupil information, images or sensitive school information to public or unapproved AI tools.

Mobile phones and personal devices

The school's default position is that the school day is mobile-phone-free for pupils. Pupils should not use or have access to personal mobile phones during the school day, including lessons, breaktimes and lunchtimes. Where a pupil is permitted to bring a phone in exceptional circumstances (for example, an agreed Year 6 travel arrangement), it must be switched off and handed to the class teacher for secure storage until the end of the day. Any exception must be agreed by the Headteacher or delegated senior leader and recorded.

Any exception required for medical, accessibility or safeguarding reasons will be agreed individually and recorded, with clear arrangements for use and storage. Personal devices are brought onto the premises at the owner's risk.

Staff personal phones must be kept out of sight and not used when supervising or teaching pupils, except where an agreed professional or emergency reason applies. School-owned devices should be used for school business wherever possible. In a genuine emergency where a school device is unavailable, a staff member may use a personal phone only as necessary, must maintain confidentiality, must not exchange personal contact details with a pupil, and must report the use to the Headteacher or DSL as appropriate. Staff must not photograph or record pupils on personal devices.

Wearable technology

Internet-enabled watches and other wearable devices must not be used by pupils during the school day. Where a pupil wears a device for an agreed medical or accessibility reason, the school will agree and record appropriate arrangements.

Staff devices used outside school

Staff must keep school devices and information secure when working away from school. Devices must be password protected, kept updated, locked when unattended and protected by appropriate security software and encryption where available. Staff must not share work devices with family or friends, store school information in personal accounts or use devices in a way that breaches the acceptable use agreement. Any loss, theft, suspected compromise or accidental disclosure must be reported immediately to the Headteacher and IT support in accordance with the school's data breach procedures.

9. Responding to online safety concerns and incidents

All online safety concerns must be taken seriously. Staff must act promptly, remain calm, listen to the pupil and report concerns to the DSL or deputy without delay. Staff must not promise confidentiality. Safeguarding concerns must be recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy, including the concern, actions taken, decisions, rationale and outcome.

The DSL will assess the concern and decide whether it requires action under the Child Protection and Safeguarding Policy, Behaviour Policy, anti-bullying procedures, staff conduct procedures or referral to an external

agency or the police. Online incidents may also require a response where the activity took place outside school but affects a pupil's safety or wellbeing in school.

The school's response will be proportionate to the nature, seriousness and circumstances of the incident. It may include supporting affected pupils, contacting parents/carers where appropriate, preserving relevant evidence safely, applying behaviour sanctions, providing education or support, reviewing risk assessments and referring to children's social care or the police.

Child-on-child online abuse and cyberbullying

Online child-on-child abuse may include abusive, harassing or discriminatory messages; threats; coercion; unwanted contact; sharing or threatening to share images; impersonation; exclusion from online groups; and the use of AI-generated or manipulated content to target another child. Such behaviour must not be dismissed as banter, a joke or an inevitable part of growing up.

The school will respond in line with its safeguarding and behaviour procedures. A single serious incident may require intervention even where it does not meet a repeated-behaviour definition of bullying. The DSL will consider the needs and safety of all children involved, including the child harmed and the child alleged to have caused harm.

Nude or semi-nude images and explicit content

If a member of staff becomes aware that a device may contain a nude or semi-nude image of a child, they must not deliberately view, copy, print, screenshot, forward or share the image. They must report the matter to the DSL immediately and follow the current DfE and UKCIS guidance. Staff must not investigate by asking a child to show them the image or by circulating it to colleagues. The DSL will decide the appropriate safeguarding response and whether advice or referral to external agencies is required.

The school will follow current DfE guidance on searching, screening and confiscation and UKCIS guidance on sharing nudes and semi-nudes. Any suspected criminal evidence must be preserved and handled in accordance with police and safeguarding advice. Staff must not delete material that may be evidence of an offence.

Misuse by staff

Concerns that a member of staff, volunteer, contractor or other adult has misused technology or acted inappropriately online must be reported and managed under the school's safeguarding allegations and low-level concerns procedures, as appropriate, and the Staff Code of Conduct. The school will consider referral to the Local Authority Designated Officer (LADO), the police or other agencies where required.

10. Searching, screening and confiscation of electronic devices

The Headteacher and staff authorised by the Headteacher may search for and confiscate electronic devices in accordance with current DfE guidance on searching, screening and confiscation, the school's Behaviour Policy and applicable law.

Before carrying out a search, the authorised member of staff must be satisfied that there are reasonable grounds and must consider urgency, the risk to pupils and staff, and whether advice from the Headteacher is required. The pupil should be given an appropriate explanation and an opportunity to cooperate, having regard to their age, understanding and needs.

Any examination of data or files must be undertaken only where permitted by current guidance and where there is a good reason. Staff must not access, copy or share suspected nude or semi-nude images of children. Where material may be evidence of an offence, staff must not delete or alter it and must seek immediate advice from the DSL and, where appropriate, the police. The DSL and Headteacher will determine next steps in line with current guidance.

Searches and confiscation must be recorded in accordance with school procedures. Complaints will be handled through the school's complaints procedure.

11. Training

All new staff will receive online safety and safeguarding training as part of induction. All staff will receive refresher training at least annually and updates when needed. Training will cover:

- current online risks and the four categories of risk;
- online child-on-child abuse, cyberbullying, grooming, exploitation and harmful content;
- AI tools, manipulated images and the risks of uploading personal or sensitive information;
- the school's filtering and monitoring arrangements, alerts and reporting procedures;
- appropriate supervision and in-person monitoring of pupils using devices;
- how to respond to disclosures and concerns, including concerns involving nude or semi-nude images; and
- professional conduct, acceptable use, data protection and secure handling of school information.

The DSL and deputies will receive safeguarding training, including online safety, in accordance with KCSIE and the school's safeguarding training arrangements, and will update their knowledge regularly. Governors will receive appropriate safeguarding and online safety training. Volunteers will receive suitable information and training for their role.

12. Monitoring, evaluation and review

The DSL and deputy DSLs will ensure online safeguarding concerns are recorded on CPOMS and reviewed for patterns, repeat concerns and emerging risks. The Headteacher and DSL will provide appropriate reports to the governing body, respecting confidentiality and data protection requirements.

This policy will be reviewed at least annually by the Deputy Headteacher in consultation with the DSL, Headteacher, IT support and safeguarding governor. It will also be reviewed sooner following significant incidents, changes to technology or working practices, or changes to statutory guidance. The governing body / Academy Council will receive the policy at each review and approve it in accordance with the Trust's scheme of delegation.

The review will consider the effectiveness of the policy, curriculum, staff training, filtering and monitoring, incident response, pupil and parent feedback, and the needs of vulnerable pupils.

13. Links with other policies and procedures

This policy should be read alongside:

- Child Protection and Safeguarding Policy;
- Child-on-child abuse policy
- Behaviour Policy and anti-bullying procedures;
- Staff Code of Conduct and staff disciplinary procedures;
- Data Protection Policy, privacy notices and data breach procedures;
- IT security / acceptable use policies and agreements for pupils, staff, governors and visitors;
- Complaints Procedure; and
- AI use guidance or policy, where adopted by the school or Trust.

This policy will be reviewed at least annually, and will be updated when relevant statutory guidance or school arrangements change.

Appendix A– Record of filtering and monitoring checks

Date	Person completing check	System / device / user group checked	Findings / issue	Action, owner and completion date

Appendix B– Online safety incident record: minimum information

Record online safety incidents on CPOMS in line with the school's safeguarding recording procedures. Records should include, where known and appropriate:

- date, time and location / platform;
- who raised the concern and who was involved;
- a factual description of what was reported or observed, using the child's words where appropriate;
- immediate actions taken and who was informed;
- DSL assessment, decisions and rationale;
- parent / carer contact and external referrals, where appropriate;
- support and safety planning for the children involved; and
- outcome, follow-up actions, responsible person and review date.