



Online Safety Policy

Safeguarding children in a connected world

Policy owner	Headteacher and Designated Safeguarding Lead
Responsible governor	Safeguarding Governor
Approved by	Local Governing Body
Policy date	September 2026
Next review	September 2027 or sooner if guidance changes
Applies to	Pupils, staff, governors, volunteers, visitors and contractors

Our Mission

“We are proud of our school as a place of learning, prayer and happiness. Hand in hand with God, Our Lady and St. Joseph, we promise to work hard and be kind to one another so that we can grow stronger together in our faith.”

Online safety is part of safeguarding. It is reflected in our culture, curriculum, technology, behaviour expectations and partnership with families.

1 Purpose and scope

St Joseph's Catholic Voluntary Academy is committed to enabling pupils to use technology safely, respectfully, responsibly and confidently. Digital technology supports learning, communication and inclusion, but may also expose children and adults to harm. The school takes a whole-school approach in which online and offline safeguarding are considered together.

This policy sets out how the school prevents, identifies and responds to online safety concerns. It applies whenever school systems, accounts, networks or devices are used and to conduct away from school where there is a safeguarding concern, an impact on pupils or staff, or a connection with the school. It should be read with the Child Protection and Safeguarding Policy, Behaviour Policy and Acceptable Use Agreements.

Nothing in this policy prevents immediate safeguarding action. Any concern about a child must be reported to the Designated Safeguarding Lead or a deputy without delay. If there is immediate danger, emergency services must be contacted.

2 Aims

- place the welfare and best interests of children at the centre of decisions;
- create a safe digital environment without unnecessarily limiting teaching and learning;
- teach pupils the knowledge, skills and judgement needed to manage online risk and seek help;
- set clear expectations for pupils, staff, governors, volunteers and visitors;
- ensure appropriate filtering and monitoring with clear safeguarding and technical oversight;
- respond consistently to online abuse, bullying, exploitation, harmful content and security incidents;
- protect personal data, images, accounts and school systems; and
- work constructively with parents, carers, the academy trust and external agencies.

3 Legal and guidance framework

This policy has regard to current legislation and national guidance, including:

- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children;
- Department for Education filtering and monitoring standards for schools and colleges;
- Department for Education guidance on teaching online safety in schools;
- UK Council for Internet Safety guidance on sharing nudes and semi-nudes;
- Education Act 2002, Children Acts 1989 and 2004 and Counter-Terrorism and Security Act 2015;
- Equality Act 2010, Human Rights Act 1998 and relevant duties to make reasonable adjustments;
- UK General Data Protection Regulation and Data Protection Act 2018;
- Computer Misuse Act 1990, Copyright Designs and Patents Act 1988 and Malicious Communications Act 1988;
- Voyeurism Offences Act 2019 and the Online Safety Act 2023 where relevant; and
- academy trust policies, local safeguarding partnership procedures and current terms of service for approved platforms.

4 Online risk

The school uses the four areas of online risk described in statutory safeguarding guidance:

Area	What it includes
Content	Being exposed to illegal, inappropriate or harmful material, misinformation or manipulated content.
Contact	Harmful interaction with other users, including adults or peers who may seek to bully, exploit, deceive or pressure a child.
Conduct	Personal online behaviour that may increase risk or harm others, including bullying, unsafe sharing, impersonation or misuse of technology.
Commerce	Risks linked to advertising, scams, in-app purchasing, financial exploitation or services unsuitable for children.

Risk may arise through websites, search, email, messaging, games, social media, live streaming, video, cloud services, connected devices, virtual or augmented reality and generative artificial intelligence. The school recognises that technology and patterns of harm change quickly.

5 Roles and responsibilities

5.1 Local Governing Body

- has strategic responsibility for online safety and appropriate filtering and monitoring;
- appoints a safeguarding governor and ensures a senior leader is responsible for the filtering and monitoring standards;
- receives assurance that systems, training, curriculum and incident response are effective;
- ensures filtering and monitoring provision is reviewed at least annually and that actions are recorded; and
- reviews this policy annually and after a serious incident or significant change in guidance or technology.

5.2 Headteacher and senior leaders

- create a safeguarding culture in which online concerns are recognised, reported and acted upon;
- allocate clear responsibilities to the DSL, IT support, curriculum leaders and staff;
- approve digital systems and services following safeguarding, privacy, security and educational checks;

- ensure staff receive induction and regular training;
- ensure incidents are managed consistently and parents, the trust and agencies are informed where appropriate; and
- make sure remote and blended learning arrangements meet the same safeguarding expectations.

5.3 Designated Safeguarding Lead

- takes lead responsibility for online safety and understands the filtering and monitoring systems in use;
- reviews relevant monitoring information and responds to safeguarding alerts;
- ensures concerns are recorded, assessed, referred and followed up under safeguarding procedures;
- works with IT support and senior leaders to review risks, patterns and training needs;
- supports pupils and families and liaises with children's social care, police and other agencies where necessary; and
- reports themes and assurance information to leaders and governors without identifying children unnecessarily.

5.4 IT support and service providers

- maintain secure networks, accounts, devices, filtering, monitoring, backups and updates;
- provide timely reports and act promptly on technical or safeguarding instructions;
- test provision after relevant changes and keep clear records of checks and actions;
- apply least-privilege access and protect administrator credentials; and
- work with the DSL and senior leadership while respecting confidentiality and data protection.

5.5 All staff and volunteers

- read and follow this policy, the safeguarding policy, staff code of conduct and acceptable use agreement;
- use only approved systems, accounts and storage for school work;
- maintain professional boundaries and use school-approved communication channels;
- provide appropriate supervision and check digital resources before use;
- never investigate a safeguarding concern themselves or forward harmful material unnecessarily;
- report concerns, mistaken access, security weaknesses and suspected data breaches promptly; and
- model respectful, lawful and responsible use of technology.

5.6 Pupils

- follow the pupil acceptable use agreement and classroom instructions;
- use school technology for agreed educational purposes;
- treat others respectfully and do not create, request, search for or share harmful or inappropriate material;
- keep passwords private and protect personal information;
- tell a trusted adult promptly about anything worrying, unsafe or accidental; and
- understand that reporting a concern is the right action and that staff will help.

5.7 Parents and carers

- support school expectations and discuss safe, respectful technology use at home;
- raise concerns promptly and preserve relevant evidence without redistributing harmful content;
- inform the school of online incidents that may affect a pupil or the school community; and
- work with the school on proportionate support, boundaries and follow-up.

6 Education and prevention

Online safety is taught through Computing, Relationships and Health Education, PSHE, Religious Education and relevant learning across the curriculum. Teaching is age-appropriate, progressive and revisited. It develops safe habits, critical thinking, digital citizenship and confidence to seek help.

Pupils learn about privacy, passwords, respectful communication, reliable information, copyright, scams, persuasive design, healthy technology habits, reporting tools and the lasting impact of online choices. Teaching also addresses harmful contact and conduct in an age-appropriate way without placing responsibility for abuse on the child.

Staff consider current local and national concerns, pupil voice and lessons from incidents. Resources are checked before use. Visitors and external programmes are appropriately vetted and their work forms part of, rather than replaces, the planned curriculum.

7 Inclusion and adaptive teaching

Every pupil should be able to understand and apply online safety learning. Some children may face additional risk because of age, SEND, communication needs, EAL, care experience, social isolation, trauma, disadvantage or limited digital access. Additional vulnerability never reduces a child's right to access suitable technology and learning.

Adaptive approaches may include pre-teaching vocabulary, visual prompts, social stories, explicit modelling, repetition, supported practice, accessible reporting routes, carefully chosen examples and work with families and professionals. The school will make reasonable adjustments while maintaining high safeguarding expectations.

8 Filtering and monitoring

The school uses filtering to restrict access to illegal, inappropriate and harmful content and monitoring to identify activity that may require action. These controls support, but do not replace, effective supervision, education, professional curiosity and clear reporting procedures. No system can remove every risk.

The Local Governing Body has overall strategic responsibility. A named senior leader and safeguarding governor oversee assurance. The DSL leads safeguarding decisions and reviews relevant reports. IT support maintains the technical provision and completes agreed checks and actions.

The school will:

- review filtering and monitoring provision at least once each academic year and when risk, working practices, devices, software or technology change;
- consider the age, SEND, EAL and safeguarding profile of pupils and the way technology is used;
- document what is blocked or allowed, the reason for decisions and the process for authorised exceptions;
- check that controls operate on school-managed devices, services, user groups and relevant locations;
- keep a log of the date, person, tests, findings and actions from checks;
- make sure alerts and reports reach people able to respond promptly;
- test new devices and services before deployment and after significant changes; and
- balance protection with legitimate teaching, learning, accessibility and safeguarding needs.

Requests to unblock content must follow the approved process. Staff must not attempt to bypass controls. A safeguarding concern revealed through monitoring will be handled under the Child Protection and Safeguarding Policy; a technical issue will be escalated to IT support and senior leadership.

9 School accounts devices and network security

- Each user must use their own authorised account and must not disclose or reuse school passwords inappropriately.
- Multi-factor authentication will be used where required or available for sensitive and privileged accounts.
- Devices must be locked when unattended and stored, transported and charged safely.
- Software, browser extensions, apps and cloud services must not be installed or connected without approval.
- Security updates, malware protection, backups and access controls will be managed by authorised staff.

- Personal USB storage or other removable media may be used only where expressly approved and securely managed.
- Suspected compromise, phishing, loss, theft or accidental disclosure must be reported immediately and must not be concealed.
- School systems may be logged and monitored for safeguarding, security and operational purposes in a lawful and proportionate way.

10 Personal devices and mobile phones

Pupil mobile phones and personal connected devices must be switched off and stored in accordance with the school's current rules. They must not be used during lessons, social times, clubs or visits unless a member of staff has given specific permission for a defined educational, medical or accessibility purpose. Smart watches and wearable devices are included where their functions create the same risks.

Staff personal devices must not be used to photograph, record or communicate privately with pupils. Personal phones should be stored and used only in staff-designated areas, except where authorised for an emergency, approved school process or reasonable adjustment. Visitors and contractors will follow the instructions given on arrival.

The school may investigate and apply its behaviour or safeguarding procedures where personal-device use affects safety, wellbeing, learning, staff or the reputation and orderly running of the school. Searching or examining a device will only occur where lawful, necessary and in line with the school's searching and safeguarding procedures.

11 Communication social media and professional boundaries

School communication with pupils and families must take place through approved accounts and platforms. Staff must not use personal messaging, personal email or personal social-media accounts to contact pupils. Staff must maintain appropriate privacy settings but recognise that online activity may still become public.

- Do not publish confidential information, pupil work, images or school matters without authority.
- Do not accept or initiate pupil connections through personal social-media accounts.
- Do not discuss individual pupils, families or colleagues online.
- Do not post material that undermines professional responsibilities or safeguarding expectations.
- Report impersonation, harassment, threatening communication or boundary concerns to the Headteacher or DSL.
- Use official school channels for public statements and media enquiries.

12 Images video and live or recorded learning

Images and recordings of pupils are personal data and must be created, stored, shared and deleted for a clear school purpose. The school will provide families with transparent information and identify the appropriate lawful basis. Consent will be obtained where consent is the correct lawful basis and may be withdrawn for future use.

Only school-approved devices, accounts and storage may be used. Staff must check relevant restrictions before publication and avoid adding unnecessary identifying information. Livestreamed or recorded learning requires approved platforms, appropriate supervision and clear expectations. Pupils must not record staff or other pupils without permission.

13 Data protection privacy and digital services

Personal data will be processed lawfully, fairly, transparently and securely. Access will be limited to those who need it. Staff must use approved storage and secure transfer methods, check recipients before sending information and report suspected personal-data breaches immediately under the Data Protection Policy.

Before introducing a platform, app, connected device or online service, the school will consider educational purpose, safeguarding, age restrictions, accessibility, privacy, security, advertising, data location and retention, account controls, contract terms and exit arrangements. A data protection impact assessment will be completed where required.

14 Generative artificial intelligence

Generative artificial intelligence can support learning and staff efficiency, but it may produce inaccurate, biased, unsafe or fabricated content and may create privacy, intellectual-property and safeguarding risks. It must therefore be used only through approved tools and for an agreed educational or operational purpose.

- Personal, confidential or special-category data about pupils, families or staff must not be entered into unapproved AI tools.
- Age requirements, product safety, filtering, monitoring, privacy and account arrangements must be checked before pupil use.
- A responsible adult must retain professional judgement; AI output must not make safeguarding, admissions, assessment or other significant decisions about a child.
- Users must check accuracy, bias, suitability and copyright and should identify AI assistance where required by the task.
- AI-generated images, audio or video must not be used to impersonate, humiliate, deceive, bully or create harmful material.
- Suspected misuse or unsafe output must be reported promptly and managed under safeguarding, behaviour, data-protection or disciplinary procedures as appropriate.

15 Responding to online safety concerns

The safety and welfare of the child come first. Staff must remain calm, listen, take the concern seriously, avoid promising confidentiality and explain that information will be shared only with people who need to help. Staff must not conduct their own investigation or ask a child to repeatedly recount events.

When a concern is reported or discovered, staff will:

- take immediate action to protect any child at risk and obtain emergency help if required;
- report the matter to the DSL or a deputy without delay and make a factual record;
- preserve relevant information safely without unnecessarily viewing, copying or forwarding harmful content;
- follow the safeguarding policy for referrals, information sharing and contact with parents or carers;
- involve police, children's social care, the academy trust, local authority or technical specialists where appropriate;
- provide proportionate support to the child or children affected and address the behaviour of those responsible;
- consider whether other pupils or adults may be at risk; and
- review lessons learned, filtering, supervision, curriculum, support and risk assessment.

Parents and carers will normally be involved unless doing so may place a child at additional risk, impede an investigation or conflict with advice from statutory agencies. Records will be stored in the appropriate safeguarding, behaviour, technical or data-protection system and cross-referenced where necessary.

16 Child on child online abuse and bullying

Online abuse between children is never dismissed as banter, part of growing up or an inevitable feature of digital life. It may occur inside or outside school and may include harassment, bullying, prejudice-based abuse, coercion, threats, impersonation, exclusion, harmful sharing or misuse of images and accounts.

The school will assess risk to all children involved, recognising that a child who has harmed another may also need safeguarding support. Responses will be child-centred, proportionate and coordinated through safeguarding and behaviour procedures. Support will not depend on a criminal threshold being met.

17 Sharing nudes and semi nudes

Concerns involving the sharing of nudes or semi-nudes by children will be managed by the DSL in line with current UK Council for Internet Safety guidance. Staff must not view, copy, print, save, forward or ask a child to send an image. A device should not be confiscated merely to search for such material unless this is directed through an authorised and lawful process.

The DSL will complete an immediate risk assessment, consider the needs of all children involved, decide whether external agencies are required and record the rationale for decisions. Parents or carers will normally be

informed unless this would increase risk to a child. The focus will be safeguarding, education and support, with behaviour consequences considered proportionately.

18 Online sexual harassment exploitation and grooming

Any concern that a child is being pressured, manipulated, exploited, groomed or sexually harassed online is a safeguarding matter and must be reported immediately to the DSL. Staff will not confront a suspected perpetrator or alert them to the concern. The DSL will follow safeguarding partnership procedures and seek police or children's social care advice where appropriate.

19 Harmful content misinformation and radicalisation

Pupils are taught to question the reliability, purpose and source of online information and to recognise manipulated or AI-generated content. Staff will respond sensitively where a pupil encounters distressing or harmful material and will assess whether safeguarding action is required.

Concerns about extremist influence or radicalisation will be reported to the DSL and managed under the Prevent risk assessment and safeguarding procedures. Legitimate discussion, curiosity and protected beliefs must not be confused with risk; decisions will be proportionate and based on evidence and context.

20 Remote education and learning away from school

Remote learning will use approved platforms, accounts and resources. Staff will follow professional boundaries, appropriate times, dress and locations, and will avoid one-to-one live sessions unless specifically authorised, risk assessed and arranged with suitable safeguards. Where possible, a parent or carer should know that a session is taking place.

Pupils and families must not record or redistribute lessons without permission. Concerns arising during remote learning will be reported and managed in the same way as concerns in school. The school will consider accessibility, digital exclusion and reasonable adjustments when planning remote provision.

21 Sanctions support and restoration

Responses will consider intent, impact, age, understanding, vulnerability, SEND, repetition, coercion and the need to protect others. Safeguarding support and disciplinary action may occur together. The school will avoid approaches that shame a child or discourage future reporting.

Possible responses include education, restorative work where safe, parental involvement, increased supervision, changes to access, pastoral or SEND support, risk assessment, sanctions under the Behaviour Policy and referral to external agencies. Restrictions will be reviewed and should be no broader or longer than necessary.

22 Staff concerns allegations and low level concerns

Any concern about an adult's online conduct, professional boundaries or use of technology must be reported under the staff code of conduct, safeguarding and allegations procedures. Concerns about the Headteacher must be reported to the Chair of Governors or academy trust as set out in those procedures. Staff must not investigate the matter themselves or discuss it widely.

23 Training information and partnership with families

All staff receive online safety and filtering and monitoring information at induction and regular updates thereafter. Role-specific training is provided for the DSL, deputies, senior leaders, governors and staff responsible for technology. Training is refreshed when risks, systems, guidance or patterns of incidents change.

Pupils are reminded regularly how to report concerns. Parents and carers receive accessible information about school expectations, emerging risks, support and reporting routes. The school will listen to pupil and parent voice while retaining professional responsibility for safeguarding decisions.

24 Monitoring review and records

The Headteacher and DSL will monitor incidents, curriculum coverage, training, filtering and monitoring information and feedback to identify patterns and improvement actions. Reports to governors will protect confidentiality and focus on assurance, trends, actions and impact.

This policy will be reviewed at least annually and sooner after a serious incident, significant change to technology, identified weakness, legal change or revised statutory guidance. The annual filtering and monitoring review is a separate recorded assurance activity and does not replace policy review.

25 Complaints

Concerns should normally be raised with the Headteacher. Formal complaints will be considered under the school's Complaints Policy. Safeguarding concerns must be reported immediately through safeguarding procedures and should not wait for the complaints process.

26 Linked policies and documents

Child Protection and Safeguarding Policy; Staff Code of Conduct; Pupil and Staff Acceptable Use Agreements; Behaviour Policy; Anti-Bullying Policy; Relationships and Health Education Policy; Computing Policy; SEND Policy and SEN Information Report; Data Protection Policy; Privacy Notices; Records Management Policy; Photography and Images Guidance; Mobile Phone Policy; Remote Education Procedures; Prevent Risk Assessment; Critical Incident and Business Continuity Plans; Whistleblowing Policy; Complaints Policy; and academy trust IT and cyber-security procedures.

27 Current guidance and support

Department for Education: Keeping Children Safe in Education 2026

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

Department for Education: Filtering and monitoring core standard

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

Department for Education: Teaching online safety in schools

<https://www.gov.uk/government/publications/teaching-online-safety-in-schools>

UK Council for Internet Safety: Sharing nudes and semi-nudes guidance

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

National Cyber Security Centre: Cyber security guidance for schools

<https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>

Childline: Online and mobile safety support

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/>

CEOP: Report online sexual abuse or grooming concerns

<https://www.ceop.police.uk/Safety-Centre/>