

ST JOHN FISHER CATHOLIC PRIMARY SCHOOL

Online Safety Policy



***“With God’s Love we are a family:
Caring, Learning and Growing together”***

	Name of School	St John Fisher Catholic Primary
	Policy Review Date	October 2026
	Date of Next Review	October 2027
	Who reviewed this policy?	Head Teacher and Governors

Designated Safeguarding Lead (DSL)	Mrs Dickinson – Headteacher
Deputy DSL	Mrs Harrison – Deputy Headteacher
Deputy DSL	Mrs Smith – Pastoral Lead
Online Safety / Computing Lead	Mrs Harrison – Deputy Headteacher

1. Purpose and Catholic ethos

At St John Fisher Catholic Primary School, online safety is an essential part of safeguarding and of preparing pupils to participate confidently, responsibly and compassionately in a digital world. Our mission calls us to care for one another, make wise choices, respect the dignity of every person and use technology in ways that help our school family to learn and grow together.

We recognise that technology provides significant opportunities for learning, communication, creativity and inclusion, while also creating potential risks. The school takes a child-centred, proportionate approach that seeks to protect pupils from harm while teaching them the knowledge, skills and judgement needed to manage online risks.

2. Scope

This policy applies to pupils, staff, governors, volunteers, visitors and contractors and to the use of school-owned and personal devices, school systems, networks, internet access, cloud services, online learning platforms, social media, messaging, artificial intelligence and other digital technologies where their use affects the school community.

Online safety incidents may occur inside or outside school. Where an incident affects the welfare of a pupil or the safe operation of the school, the school will respond in accordance with safeguarding, behaviour, staff conduct and other relevant procedures.

3. Statutory and guidance framework

This policy reflects current statutory and national guidance, including Keeping Children Safe in Education 2026 (KCSIE), the DfE filtering and monitoring core standard, DfE digital and technology standards, the Prevent duty, the Data Protection Act 2018 and UK GDPR as amended, the Data (Use and Access) Act 2025, the Education Act 2011, the Computer Misuse Act 1990 and current DfE guidance on generative artificial intelligence in education.

KCSIE 2026 makes clear that safeguarding children online is part of the school's statutory safeguarding responsibilities and that governing bodies and proprietors should ensure appropriate filtering and monitoring systems are in place.

2026 update – key current requirements

The school will keep its online-safety arrangements under review in light of current statutory guidance and DfE standards. In particular:

- Filtering and monitoring will be reviewed at least annually, with clear responsibility for reviewing alerts and escalating safeguarding concerns.
- The school will understand the coverage and limitations of its filtering and monitoring systems and will not rely on technical controls as a substitute for supervision, teaching or professional judgement.
- Filtering and monitoring arrangements will be proportionate and lawful, with access to monitoring information restricted to authorised staff.
- Any significant change to filtering or monitoring systems will consider data-protection requirements and, where appropriate, a Data Protection Impact Assessment.

- The school's mobile-phone arrangements will reflect the statutory DfE guidance which schools should follow from 1 September 2026, including appropriate exceptions and reasonable adjustments.
- Any pupil-facing generative AI use will comply with age restrictions and have appropriate supervision, safety and filtering/monitoring safeguards.
- The revised statutory Relationships Education and Health Education guidance in force from 1 September 2026 will inform the school's online-safety curriculum.

4. The four areas of online safety risk

In line with KCSIE, the school recognises online safety risks across four broad areas:

- Content – being exposed to illegal, inappropriate or harmful material, including pornography, misinformation, disinformation, misogyny, racism, self-harm, suicide, eating-disorder content, extremism and harmful AI-generated material;
- Contact – harmful interaction with other users, including peer pressure, adults posing as children, grooming, exploitation and contact from individuals seeking to radicalise or abuse;
- Conduct – personal online behaviour that increases the likelihood of harm, including cyberbullying, sharing intimate images, creating or sharing harmful content and poor digital behaviour;
- Commerce – risks such as online gambling, inappropriate advertising, phishing, scams and financial exploitation.

5. Roles and responsibilities

5.1 Governing Body

- ensure online safety is treated as part of the school's safeguarding responsibilities;
- ensure appropriate filtering and monitoring systems and processes are in place and are reviewed at least annually;
- ensure roles and responsibilities for filtering and monitoring are clearly assigned;
- ensure staff receive appropriate safeguarding and online-safety training;
- receive assurance that online-safety risks, emerging technologies and cyber-security arrangements are appropriately managed;
- ensure this policy and related safeguarding arrangements are reviewed regularly.

5.2 Headteacher

- provide leadership for a whole-school culture of safe and responsible technology use;
- ensure this policy is implemented and understood;
- ensure adequate resources, training and technical support are available;
- ensure significant online-safety incidents are managed and escalated appropriately.

5.3 DSL and Deputy DSLs

The DSL has lead responsibility for online safety within safeguarding arrangements, supported by the Deputy DSLs. They will understand the filtering and monitoring systems and processes in place and respond to online safeguarding concerns in accordance with the Safeguarding and Child Protection Policy.

- ensure online concerns are recorded, assessed and acted upon;
- consider whether early help, children's social care, police or other agencies should be involved;
- ensure online harms are considered alongside offline safeguarding information;
- work with curriculum, IT and pastoral staff to identify patterns and emerging risks.

5.4 Online Safety / Computing Lead

- support a progressive online-safety curriculum;
- promote staff, pupil and parent awareness;
- liaise with the DSL and technical support about emerging risks;
- support reviews of resources, platforms and digital practice.

5.5 All staff

All staff must read KCSIE 2026 Part One in full and follow the school's safeguarding procedures. Staff must understand that safeguarding is everyone's responsibility and that online concerns require the same professional curiosity and timely response as offline concerns.

- model safe, responsible and professional use of technology;
- supervise pupils appropriately when technology is used;
- report online safeguarding concerns to the DSL or Deputy DSL without delay;
- follow the Staff Code of Conduct and Acceptable Use arrangements;
- never investigate a safeguarding concern themselves beyond what is necessary to establish immediate safety and report it.

5.6 Pupils

Pupils are expected, at an age-appropriate level, to follow school rules for technology, behave respectfully online, protect personal information and passwords, report upsetting or unsafe experiences and seek adult help when needed.

5.7 Parents and carers

The school will work in partnership with parents and carers, providing information and guidance to help families support safe, healthy and age-appropriate technology use.

6. Online safety education

Online safety will be taught through a planned, age-appropriate and progressive curriculum, including computing and PSHE and other relevant curriculum areas. Teaching will be revisited regularly because technologies and risks change.

- privacy, personal information and digital footprints;
- passwords, account security and scams;
- healthy relationships and respectful online communication;
- cyberbullying and how to seek help;
- reliable information, misinformation and disinformation;
- age restrictions and appropriate online services;
- gaming, social media, messaging and live streaming;
- image sharing and consent;
- online grooming, exploitation and manipulation;
- extremism and radicalisation;
- commercial risks, advertising, in-app purchases and scams;
- AI-generated content, deepfakes and critical evaluation of AI outputs;
- healthy screen use and digital wellbeing;
- how and where to report concerns.

Teaching will avoid frightening or blaming pupils and will emphasise that children should tell a trusted adult if something online worries them, even if they have made a mistake.

7. Filtering

The school will maintain an active, well-managed filtering system designed to block illegal, inappropriate and harmful content without unreasonably restricting teaching and learning.

The school recognises that no filtering system is completely effective. Filtering therefore forms one part of a wider safeguarding approach that includes supervision, education, staff vigilance, reporting systems and monitoring.

- filtering will apply to school-managed internet access and devices as appropriate;
- systems will be configured according to the school's age range, safeguarding needs and risk profile;
- changes or exceptions will be authorised and documented appropriately;
- filtering effectiveness and limitations will be understood and reviewed;
- the filtering provision will be reviewed at least annually and following significant change or concern.

8. Monitoring

The school will maintain appropriate monitoring processes to identify potentially harmful or concerning activity on school systems and devices. Monitoring arrangements will be proportionate, lawful and transparent.

- roles for reviewing alerts or reports will be clearly assigned;
- urgent safeguarding concerns will be referred immediately to the DSL or Deputy DSL;
- monitoring will not replace staff supervision or professional judgement;
- staff will understand how concerns identified through monitoring should be handled;
- privacy and data-protection implications will be considered.

The annual review should be informed by the school's wider safeguarding and online-safety risk assessment, including emerging technologies and risks identified through incidents, pupil voice, parent feedback and technical monitoring.

9. Annual filtering and monitoring review

The school will review its filtering and monitoring provision at least annually. The review will involve relevant safeguarding, leadership and technical personnel and will consider the school's risk profile, pupil needs, incidents, system effectiveness, limitations, emerging technology and any required improvements.

The Governing Body will receive appropriate assurance about the outcome of the review.

10. Mobile phones and personal devices

Pupil use of mobile phones and personal devices on the school site will follow the school's agreed arrangements. The DfE's statutory mobile-phone guidance became effective for schools from 1 September 2026. The school's arrangements will prohibit use throughout the school day except where a permitted exception or agreed reasonable adjustment applies.

Staff personal-device use must comply with the Staff Code of Conduct and safeguarding expectations. Personal devices must not be used to photograph, video or communicate with pupils except where explicitly authorised under an approved school arrangement.

11. School devices, accounts and passwords

- users must use only accounts and access permissions provided or approved for them;
- passwords must not be shared and must meet school security requirements;
- multi-factor authentication will be used where required or appropriate;

- users must not attempt to bypass security, filtering or monitoring controls;
- school devices must be locked or secured when unattended;
- lost, stolen or compromised devices/accounts must be reported immediately;
- software must only be installed or used in accordance with school IT arrangements.

12. Social media and communication

Staff must maintain professional boundaries in all digital communication. Staff must not use personal social-media accounts or personal messaging services to communicate privately with pupils.

Official school communication channels should be used for school business. Staff should consider privacy, confidentiality, safeguarding and professional reputation before posting or sharing content relating to the school.

Online bullying, harassment, discriminatory abuse, impersonation or threatening behaviour affecting members of the school community will be addressed through safeguarding, behaviour or staff procedures as appropriate.

13. Photographs, video and live streaming

Images and recordings of pupils are personal data and will be handled in accordance with the school's Data Protection Policy and privacy arrangements. The school will use an appropriate lawful basis and will obtain consent where consent is the correct legal basis.

Staff will use school-approved devices and systems for school images. Images must not be stored on personal devices unless an expressly authorised school arrangement applies.

Live streaming or video conferencing involving pupils will only use approved platforms and appropriate safeguarding controls.

14. Generative artificial intelligence (AI)

The school recognises that generative AI can support teaching and administration but can also create safeguarding, privacy, accuracy, bias, intellectual-property and misinformation risks. Any use must comply with safeguarding, data-protection and school technology requirements.

- only school-approved AI tools may be used for school business where personal or confidential information could be involved;
- staff should not enter identifiable pupil, family or staff personal data into open or unapproved AI tools;
- age restrictions and supplier terms must be checked before pupils use an AI tool;
- pupil-facing AI use must be appropriately supervised and have suitable safety, filtering and monitoring safeguards;
- AI-generated content must be checked critically for accuracy, bias, appropriateness and safeguarding risks;
- AI must not replace professional judgement or the teacher-pupil relationship;
- pupils will be taught that AI can produce convincing but false or harmful information, manipulated images and deepfakes.

Where new AI tools are considered, the school will take account of DfE generative AI product safety standards, data-protection requirements and the need for risk assessment or a Data Protection Impact Assessment where appropriate.

AI tools must not be used to make or support Prevent referrals or to generate wording for a Prevent referral. Staff must follow the approved safeguarding and Prevent referral process.

15. Cyber security

Cyber security is an important part of safeguarding because disruption, data loss or unauthorised access can place pupils and staff at risk. The school will work towards and maintain appropriate DfE digital and technology standards.

- systems and software will be kept appropriately patched and updated;
- accounts will use appropriate authentication and access controls;
- backups will be maintained and protected;
- phishing, suspicious messages and suspected compromise must be reported promptly;
- users must not knowingly introduce malware or attempt unauthorised access;
- the school will maintain appropriate incident-response arrangements.

16. Data protection and privacy

Online services, apps, EdTech and AI tools must be assessed appropriately before use where they process personal data. The school will comply with its Data Protection Policy, privacy notices and relevant legislation.

Data protection law is not a barrier to appropriate safeguarding information sharing. Where information must be shared to protect a child, staff should follow safeguarding procedures and record decisions appropriately.

17. Remote and online learning

Where remote or online learning is used, school safeguarding expectations continue to apply. Approved platforms and accounts will be used, professional boundaries maintained and pupils and families given clear expectations about appropriate participation.

Any concern arising during remote learning must be reported through normal safeguarding routes.

18. Online bullying and child-on-child abuse

Online bullying and technology-assisted child-on-child abuse will be treated seriously. This can include abusive messages, exclusion, harassment, sexualised behaviour, sharing images without consent, impersonation, coercion and harmful content creation.

Incidents will be considered under the Safeguarding and Child Protection Policy and Behaviour and Relationships Policy. The school will consider the needs and safety of all children involved.

19. Sharing Nude or Semi-Nude Images

Although incidents involving nude or semi-nude images may be less common in a primary school, children can still be exposed to, receive or be encouraged to share inappropriate images online.

If the school becomes aware of any incident involving a child creating, receiving, requesting or sharing a nude or semi-nude image, staff must report the concern **immediately to the Designated Safeguarding Lead (DSL) or a Deputy DSL**.

Staff must **not ask a child to send, forward, print, download or display an image**. Staff should not intentionally view, copy or save such an image unless specifically required as part of an authorised safeguarding process.

The child's welfare will remain the school's primary concern. Incidents will be managed sensitively and in accordance with current safeguarding guidance.

20. Online Sexual Harassment, Grooming and Exploitation

Children may encounter inappropriate behaviour online, including unwanted messages, requests for personal information or images, sexualised content, grooming or contact from unsafe adults or other children.

Any concern that a pupil may be experiencing **online grooming, sexual harassment, coercion, exploitation or inappropriate contact** must be treated as a safeguarding concern and reported immediately to the DSL or Deputy DSL.

Children will be taught, in an age-appropriate way, that they should tell a trusted adult if anyone online makes them feel worried, uncomfortable, frightened or pressured.

Where appropriate, the DSL will consider whether further support or referral to Children's Social Care, the police or other specialist services is required.

21. Radicalisation and Extremism

St John Fisher Catholic Primary School will fulfil its responsibilities under the **Prevent duty** as part of its wider safeguarding arrangements.

Through age-appropriate teaching, pupils will learn that information found online is not always reliable and that some individuals or groups may attempt to influence, manipulate or encourage harmful attitudes or behaviour.

Any concern that a child may be exposed to extremist material, inappropriate influence or possible radicalisation will be reported immediately to the DSL or Deputy DSL and managed in accordance with the school's safeguarding and Prevent procedures.

22. Harmful Content, Self-Harm and Suicide

Children may accidentally or deliberately encounter upsetting or harmful material online. This may include content relating to self-harm, suicide, eating disorders, violence or other behaviour that could place a child at risk.

If a pupil accesses, searches for, receives or shares such material, staff will respond with sensitivity and recognise that this may indicate a **safeguarding or wellbeing need**, rather than treating the incident solely as a behaviour matter.

The concern must be reported to the DSL or Deputy DSL, who will consider the individual circumstances of the child and whether additional pastoral support, parental involvement or referral to another service is required.

23. Online Scams, Gaming and Commercial Risks

As part of the school's online safety curriculum, pupils will be taught how to recognise and respond to common online financial and commercial risks in an **age-appropriate way**.

This will include learning about scams, suspicious messages and links, phishing, in-app purchases, gaming purchases, loot boxes, advertising and attempts to persuade children to spend money or share personal information.

Pupils will be encouraged to **stop and ask a trusted adult** before clicking unfamiliar links, making online purchases, sharing financial information or responding to messages offering prizes, rewards or free items.

Where the school becomes aware that a pupil may have experienced significant financial exploitation, fraud or another safeguarding concern online, this will be reported to the DSL or Deputy DSL and appropriate action will be taken.

24. Reporting and responding to concerns

Pupils are encouraged to tell any trusted adult if something online makes them feel worried, frightened, pressured, embarrassed or unsafe.

Staff who become aware of an online safeguarding concern must:

- act promptly and prioritise the child's immediate safety;
- listen without blame or judgement;
- avoid promising confidentiality;
- do not conduct their own investigation;
- preserve relevant information without unnecessarily viewing or forwarding harmful content;
- report the concern to the DSL or Deputy DSL without delay;
- make an accurate safeguarding record in accordance with school procedures;
- call 999 if a child is in immediate danger.

25. Online incidents involving staff

Any online concern or allegation involving a member of staff, supply staff member, volunteer or contractor must be managed under KCSIE 2026 and the school's allegations/low-level concerns procedures. Staff must report such concerns in accordance with the Safeguarding and Child Protection Policy and Staff Code of Conduct.

26. Sanctions and support

Where a pupil misuses technology, the school will apply its Behaviour and Relationships Policy fairly and proportionately. The response will consider the pupil's age, SEND, vulnerability, intent, impact and safeguarding context.

A sanction will not replace safeguarding action. Pupils affected by online harm will be offered appropriate pastoral support and, where necessary, external support.

27. Staff training

Online safety will form part of safeguarding induction and regular safeguarding updates. Training will include current online risks, reporting routes, filtering and monitoring responsibilities, professional boundaries, cyber security and relevant developments such as AI.

28. Parent and carer engagement

The school will provide parents and carers with accessible online-safety information through the website, newsletters, workshops, alerts or other communications. Guidance will encourage open conversations at home, age-appropriate boundaries, privacy settings, healthy technology habits and early reporting of concerns.

29. Monitoring, evaluation and review

The DSL, Headteacher, Online Safety/Computing Lead and technical support will review incidents and emerging trends to identify any changes needed to curriculum, filtering, monitoring, staff training or parent information.

The Governing Body will review this policy annually and sooner following significant incidents, changes to statutory guidance, major technological change or where monitoring indicates that arrangements need strengthening.

30. Related policies

- Safeguarding and Child Protection Policy;
- Behaviour and Relationships Policy;
- Staff Code of Conduct;
- Data Protection Policy;
- Acceptable Use Agreements;
- Anti-Bullying Policy;
- RSHE / PSHE Policy;
- Computing Policy;
- Mobile Phone / Personal Device arrangements;
- Photography and Video arrangements;
- Cyber Security / IT procedures;
- Prevent procedures.

Appendix 1 – Online safety responsibilities at a glance

Role	Key responsibility	Action
Governing Body	Strategic safeguarding oversight	Assure filtering/monitoring, training and annual review
Headteacher	Whole-school implementation	Resources, culture, procedures and escalation
DSL / Deputy DSLs	Online safeguarding	Receive, assess, record and refer concerns
Online Safety / Computing Lead	Curriculum and awareness	Progressive teaching and emerging-risk updates
Technical support	Technical controls	Maintain systems, filtering, monitoring and cyber controls

All staff	Safeguarding and supervision	Model safe use and report concerns immediately
Pupils	Safe and respectful use	Follow rules and tell a trusted adult
Parents/carers	Partnership	Support safe use and raise concerns early

Appendix 2 – Filtering and monitoring annual review checklist

- Are roles and responsibilities clearly identified and understood?
- Does filtering reflect the age, needs and risk profile of our pupils?
- Does filtering block harmful content without unreasonably restricting learning?
- Do we understand the limitations of our filtering system?
- Are monitoring alerts/reports reviewed by appropriate trained staff?
- Are urgent safeguarding alerts escalated promptly to the DSL?
- Are school devices, users and relevant networks covered appropriately?
- Have significant incidents or attempted breaches identified any gaps?
- Have AI and new EdTech tools changed our risk profile?
- Are staff, pupils and governors aware of relevant arrangements?
- Are actions from the previous review complete?
- Have findings and required improvements been reported appropriately to governors?

Appendix 3 – Pupil online safety rules

- I use technology for the purpose my teacher has agreed.
- I keep passwords and personal information private.
- I am kind and respectful when I communicate online.
- I do not try to bypass school safety or filtering systems.
- I ask before taking or sharing photographs or videos.
- I check information carefully and remember that online and AI-generated content may not be true.
- I tell a trusted adult straight away if I see something upsetting, unsafe or inappropriate.
- I know I can ask for help even if I clicked something by mistake or made a poor choice.

Key current guidance and resources

- Keeping Children Safe in Education 2026 – Department for Education.
- DfE Filtering and monitoring: core standard and Cyber security: core standard.
- Mobile phones in schools – statutory DfE guidance, to be followed from 1 September 2026.
- Relationships Education, Relationships and Sex Education (RSE) and Health Education – statutory guidance in force from 1 September 2026.
- Teaching online safety in schools – Department for Education.
- Generative artificial intelligence (AI) in education and Generative AI: product safety standards – Department for Education.
- Data protection in schools – Department for Education.
- Prevent Duty Guidance: England and Wales (2023).
- Sharing nudes and semi-nudes: advice for education settings.