When you love to learn, you learn to love

Online Safety Policy

Date of Review	November, 2026
Agreed by Governors	November, 2026
Shared with all Staff	November, 2026
Next Review	September, 2027

Contents

1. Our Catholic Ethos and Commitment to Online Safety..... 3

2.Aims and Scope of the Policy..... 3

3. Legislation and Guidance 5

4. Roles and Responsibilities.....5

5. Teaching and Learning: Developing Digital Responsibility.....9

6. Understanding and Managing Risks Online 11

7. Filtering and Monitoring.....13

8. Use of Devices and Technology in School 15

9. Mobile Phones, Smart Devices and Personal Technology.....17

10. Staff Conduct and Online Communication.....19

11. Social Media and Published Content.....20

12. Online Safety Incidents and Safeguarding Responses 21

13. Data Protection, Privacy and Information Security.....24

14. Remote Learning and Online Meetings.....25

15. Working in Partnership with Parents and Carers.....25

16. Staff Training and Awareness 26

17. Monitoring, Evaluation and Policy Review.....26

- Appendix 1: Pupil Acceptable Use Agreement.....28

1. Our Catholic Ethos and Commitment to Online Safety

Our Mission

We stand united in our mission to build a loving world of truth, justice, peace and wisdom.

At St John Fisher Catholic Primary School, we believe that every child is made in the image and likeness of God and has the right to feel safe, valued and respected. Our Catholic faith underpins everything we do, including the way we teach children to use technology and interact with others in the digital world.

Our LIGHT values of Love, Integrity, Growth, Hope and Togetherness guide the choices we make, both online and offline. We encourage children to treat others with kindness, act with honesty, respect the dignity of every person and take responsibility for their actions.

We recognise that technology provides valuable opportunities for learning, communication, creativity and personal development. However, the online world also presents risks, and children may encounter harmful or inappropriate content, contact or behaviour, sometimes without fully understanding the consequences.

We are committed to protecting children from online harm, developing their understanding of how to use technology safely and responsibly, and ensuring that they know how to seek help when something makes them feel uncomfortable or unsafe.

Online safety is an integral part of our safeguarding culture. It is the responsibility of everyone in our school community, including governors, staff, volunteers, parents and pupils. We work in partnership to ensure that children are supported in developing the knowledge, confidence and judgement they need to navigate an increasingly digital world.

2. Aims and Scope of the Policy

The purpose of this policy is to establish a consistent approach to online safety across St John Fisher Catholic Primary School. It sets out how we protect pupils, staff and the wider school community when using digital technology and how we respond when concerns arise.

We aim to:

- Provide a safe and secure digital environment in which technology can be used to support high-quality teaching and learning.
- Protect pupils from online abuse, exploitation, inappropriate content and other forms of digital harm, both in school and beyond.
- Develop children's understanding of online risks and their ability to make safe, informed and responsible choices.
- Ensure that pupils understand how to behave respectfully online and recognise that the same standards of kindness, honesty and respect apply in the digital world as they do in everyday life.
- Ensure that all staff understand their safeguarding responsibilities and know how to recognise, report and respond to online safety concerns.
- Maintain effective filtering and monitoring arrangements and ensure that concerns identified through these systems are acted upon.
- Promote the safe and appropriate use of school devices, online platforms, communication systems and emerging technologies, including artificial intelligence.
- Work constructively with parents and carers to reinforce consistent messages about online safety.
- Meet our statutory safeguarding, data protection and information security responsibilities.

This policy applies to all members of the school community and covers the use of technology on school premises, school devices and networks, school-managed accounts and platforms, and any online activity outside school that has an impact on the safety, welfare or relationships of pupils or members of the school community.

It applies to all staff, including teaching staff, support staff, supply staff, volunteers, governors, contractors and visitors where relevant.

The policy should be read alongside the school's:

- Child Protection and Safeguarding Policy.
- Behaviour Policy.
- Anti-Bullying Policy.
- Staff Code of Conduct.
- Staff and Pupil Acceptable Use Agreements.
- Data Protection Policy.

- Whistleblowing Policy.

3. Legislation and Statutory Guidance

This policy has been developed with regard to current legislation and statutory and non-statutory guidance, including:

- Keeping Children Safe in Education (2026).
- Working Together to Safeguard Children (2023, as subsequently updated).
- Education Act 2002.
- Education Act 2011.
- Children Act 1989 and Children Act 2004.
- Equality Act 2010.
- Data Protection Act 2018 and UK General Data Protection Regulation.
- Protection of Children Act 1978 and Sexual Offences Act 2003, where relevant to online image-sharing offences.
- Counter-Terrorism and Security Act 2015 and the Prevent Duty Guidance.
- DfE Teaching Online Safety in Schools guidance.
- DfE Meeting Digital and Technology Standards in Schools and Colleges, including the Filtering and Monitoring Core Standard.
- DfE Generative AI: Product Safety Standards.
- UK Council for Internet Safety (UKCIS) guidance, including guidance on sharing nudes and semi-nudes.
- Bexley Safeguarding Children Partnership procedures.

The school will have regard to changes in legislation and statutory guidance and will update its arrangements accordingly.

4. Roles and Responsibilities

Online safety is a shared safeguarding responsibility. However, clear leadership and accountability are essential to ensure that the school's arrangements are effective and that concerns are dealt with promptly.

4.1 Governing Body

The Governing Body has strategic oversight of online safety and is responsible for ensuring that appropriate arrangements are in place to safeguard pupils when using technology.

Governors will:

- Ensure that online safety forms part of the school's wider safeguarding arrangements.
- Ensure that appropriate filtering and monitoring systems are in place and that their effectiveness is reviewed at least annually.
- Ensure that roles and responsibilities for managing filtering and monitoring are clearly identified.
- Receive appropriate information about online safety incidents, emerging risks and the effectiveness of the school's arrangements.
- Ensure that the school has appropriate policies, procedures and staff training in place.
- Hold the Headteacher to account for the implementation of this policy.

4.2 Headteacher

The Headteacher has overall responsibility for implementing this policy and ensuring that online safety is embedded within the school's safeguarding culture.

The Headteacher will:

- Ensure that online safety arrangements are implemented consistently across the school.
- Ensure that staff understand their responsibilities and receive appropriate training.
- Ensure that suitable filtering and monitoring arrangements are maintained in partnership with the school's technical support provider.
- Ensure that concerns are investigated and addressed in accordance with safeguarding procedures.
- Ensure that parents are informed and involved where appropriate.
- Report significant concerns and relevant developments to the Governing Body.
- Ensure that the policy is reviewed regularly and updated in response to changes in technology, legislation and safeguarding practice.

4.3 Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) has responsibility for overseeing online safety concerns as part of the school's wider safeguarding arrangements.

The DSL will:

- Act as the main point of contact for staff reporting online safety concerns.
- Assess concerns and determine the appropriate safeguarding response.
- Ensure that concerns are recorded on CPOMS and that actions and decisions are documented.
- Liaise with parents, external agencies, the Local Authority and the police where appropriate.
- Consider whether online incidents indicate wider safeguarding concerns, including abuse, exploitation, coercion, bullying or radicalisation.
- Work with the Headteacher and technical support provider to review filtering and monitoring arrangements.
- Review relevant monitoring alerts and incidents, ensuring that concerns are followed up.
- Identify patterns or repeated concerns that may indicate a wider risk to an individual pupil or group of pupils.
- Ensure that online safety education reflects emerging risks and the needs of the children.

The DSL will work closely with the Deputy Designated Safeguarding Leads (DDSLs) to ensure that concerns can be responded to promptly.

4.4 Technical Support and Filtering and Monitoring

The school works with its technical support provider to maintain the security and effectiveness of its digital systems.

The technical support provider will:

- Maintain the school's filtering and monitoring systems in accordance with agreed requirements.
- Ensure that inappropriate and harmful websites and content are blocked as appropriate.
- Support the identification and investigation of technical alerts and concerns.
- Advise the school about emerging online threats, vulnerabilities and security risks.
- Support the maintenance and security of school devices, networks and accounts.
- Assist with the annual review and testing of filtering and monitoring arrangements.

Technical support does not replace the school's safeguarding responsibilities. Any concern that may involve a child's safety or welfare must be referred to the DSL.

4.5 All Staff

All staff have a responsibility to safeguard children from online harm and to model appropriate behaviour when using technology.

Staff must:

- Read and follow this policy and the relevant Acceptable Use Agreement.
- Complete safeguarding and online safety training as required by the school.
- Use school technology and approved platforms responsibly and for appropriate purposes.
- Maintain professional boundaries in all online communication.
- Supervise pupils appropriately when they are using digital devices.
- Report any inappropriate content, communication, behaviour or safeguarding concern to the DSL without delay.
- Report any accidental access to inappropriate material or any suspected failure of the school's filtering arrangements.
- Never assume that an online concern is outside the school's responsibility simply because it occurred beyond the school day or premises.

Staff must not investigate safeguarding concerns independently or attempt to resolve potentially serious online incidents without involving the DSL.

4.6 Pupils

Pupils are expected to use technology safely, responsibly and respectfully.

They should:

- Follow the Pupil Acceptable Use Agreement.
- Use school devices and online platforms only for the purposes directed by staff.
- Treat others with kindness and respect, remembering that words and actions online can affect people just as much as they do face to face.
- Keep personal information private.
- Never share passwords or use another person's account.
- Tell a trusted adult if something they see, hear or experience online worries them.

- Never deliberately access, share or create inappropriate or harmful content.
- Respect the work, privacy and personal information of others.

Children will be encouraged to understand that they will not be in trouble for asking for help or reporting something that has made them feel uncomfortable.

4.7 Parents and Carers

Parents and carers play an important role in supporting children to use technology safely beyond the school environment.

We ask parents and carers to:

- Talk regularly with their children about their online experiences.
- Be aware of the websites, games, apps and platforms their children use.
- Apply appropriate parental controls and age restrictions.
- Monitor children's use of devices, particularly where children have independent access to the internet.
- Encourage children to speak to a trusted adult if something online causes concern.
- Reinforce the importance of kindness, respect and responsible behaviour online.
- Inform the school if they become aware of online activity that may affect the safety or wellbeing of a pupil or member of the school community.

Parents should raise concerns with the school rather than attempting to resolve incidents through online exchanges or social media.

5. Teaching and Learning: Developing Digital Responsibility

At St John Fisher, online safety education is an ongoing part of our curriculum and wider personal development provision. It is not limited to an annual themed week or an isolated Computing lesson.

We recognise that children need repeated opportunities to learn about online safety as their understanding develops and their access to technology changes.

Online safety is taught through the Computing curriculum, RSHE, assemblies, class discussions, prayer and reflection, and other appropriate opportunities across the school day.

Our teaching is age-appropriate and builds progressively from Reception to Year 6. It takes account of the fact that children may encounter online risks outside school, even when they do not have independent access to devices in the classroom.

Children are taught about:

Online relationships and communication

- Treating others with kindness and respect online.
- Understanding that people may not always be who they claim to be.
- Recognising inappropriate communication, pressure, manipulation and attempts to build relationships for harmful purposes.
- Knowing how to respond if someone makes them feel uncomfortable.
- Understanding that online friendships and relationships require the same care and respect as relationships in everyday life.

Personal information and privacy

- Keeping passwords and personal information secure.
- Understanding what information should and should not be shared online.
- Recognising the risks associated with sharing photographs, videos, locations and other identifying information.
- Understanding privacy settings and the importance of seeking adult guidance.

Online content and information

- Recognising that not everything seen online is true, accurate or trustworthy.
- Understanding advertising, misleading information, scams and fake content.
- Recognising inappropriate, upsetting or harmful material.
- Understanding that information and images shared online may remain accessible even after they have been deleted.

Online behaviour and cyberbullying

- Understanding the impact of unkind, threatening or discriminatory online behaviour.
- Recognising cyberbullying and knowing how to report it.
- Understanding that sharing, liking or forwarding harmful content can contribute to the harm experienced by another person.
- Knowing when to stop engaging, block or report someone and seek help from an adult.

Online risks and exploitation

- Recognising attempts by others to obtain personal information, images or contact details.
- Understanding online grooming, coercion and manipulation in an age-appropriate way.
- Recognising that people may use games, social media, messaging services and other online platforms to approach children.
- Knowing that children should never feel pressured to share images, meet someone they have met online or keep an online interaction secret from trusted adults.

Artificial intelligence and emerging technologies

- Understanding that artificial intelligence can generate text, images, audio and video that may appear convincing but are not necessarily genuine.
- Recognising the risks associated with AI-generated images, impersonation and deepfakes.
- Understanding that AI tools may produce inaccurate, misleading or inappropriate information.
- Knowing that personal information, photographs and other sensitive information should not be entered into AI tools without appropriate permission.
- Understanding the importance of using technology honestly and responsibly.

Staff will ensure that online safety education is accessible to all pupils, including children with SEND and those who may require additional support to understand online communication, recognise risk or communicate a concern.

6. Understanding and Managing Online Risks

The school recognises that online harm can take many forms and that risks may change as technology develops. These risks are considered through four broad areas: content, contact, conduct and commerce.

6.1 Content

Children may encounter material that is inappropriate, harmful or upsetting. This may include:

- Pornographic, sexually explicit or violent material.

- Content promoting self-harm, suicide, eating disorders or other harmful behaviours.
- Racist, discriminatory, extremist or radicalising material.
- Misogynistic or hateful content.
- Dangerous challenges or activities that encourage children to put themselves or others at risk.
- False, misleading or deliberately manipulative information.

The school will take appropriate steps to prevent access to harmful material through filtering and supervision. However, we recognise that no filtering system can remove every risk and that children must also be equipped to respond appropriately when they encounter something concerning.

6.2 Contact

Children may be contacted by people seeking to manipulate, exploit or harm them.

This may happen through social media, online games, chat functions, messaging services or other digital platforms.

Risks include:

- Online grooming and sexual exploitation.
- Contact from adults or older children pretending to be someone else.
- Requests for personal information or photographs.
- Attempts to move conversations to private messaging services.
- Coercion, threats, blackmail or pressure to keep secrets.
- Attempts to encourage children to meet someone they have only known online.

Any concern that a child is being targeted, groomed or exploited must be reported to the DSL immediately.

6.3 Conduct

Children may be harmed through their own or others' online behaviour.

This includes:

- Cyberbullying, harassment and threatening messages.
- Sharing private information or photographs without permission.
- Impersonation and the creation of fake accounts.

- Discriminatory, abusive or hateful communication.
- Sharing harmful or humiliating images and videos.
- Encouraging others to participate in harmful online behaviour.
- Creating or sharing AI-generated content intended to embarrass, threaten or harm another person.

The school will respond in accordance with its Behaviour Policy, Anti-Bullying Policy and safeguarding procedures.

6.4 Commerce

Children may be exposed to online financial risks, including:

- Scams and fraudulent messages.
- Inappropriate advertising and targeted marketing.
- In-app purchases and unexpected costs.
- Gambling-related content and simulated gambling.
- Attempts to obtain financial or personal information.

Children will be taught to recognise suspicious messages and understand the importance of seeking adult advice before making purchases or sharing information.

7. Filtering and Monitoring

St John Fisher Catholic Primary School recognises that effective filtering and monitoring are essential parts of its safeguarding arrangements.

The school uses LGfL filtering and monitoring provision to help protect pupils from accessing inappropriate or harmful online content when using the school's network and devices.

Filtering and monitoring serve different purposes and both are necessary.

Filtering helps prevent access to inappropriate websites, content and online services.

Monitoring helps identify potentially concerning activity, including attempts to access blocked content or searches and activity that may indicate a safeguarding concern.

The school will ensure that its arrangements are appropriate to the age and needs of its pupils and reflect the risks associated with the technology available to them.

7.1 Responsibilities

The Governing Body is responsible for ensuring that suitable filtering and monitoring arrangements are in place.

The Headteacher will oversee the implementation and effectiveness of these arrangements, working with the DSL and technical support provider.

The DSL will support the review of safeguarding-related alerts and ensure that any concerns are followed up appropriately.

Technical support will assist with the operation, maintenance and testing of the systems.

7.2 Reviewing Effectiveness

The school will review the effectiveness of its filtering and monitoring arrangements at least annually, in line with DfE guidance.

The review will consider:

- Whether filtering is working effectively across all relevant internet-connected devices and locations.
- Whether inappropriate and harmful content is being blocked.
- Whether monitoring arrangements are identifying relevant safeguarding concerns.
- Whether alerts are being reviewed and responded to appropriately.
- Whether staff understand how to report concerns and escalate technical issues.
- Whether changes in technology or pupil access create additional risks.
- Whether the school's provision remains appropriate for its age range and safeguarding needs.

Records of reviews, testing and actions taken will be maintained.

The school will ensure that staff know how to report inappropriate material, suspected breaches or concerns about the effectiveness of filtering.

7.3 Responding to Alerts

Where monitoring identifies potentially concerning activity, the school will consider the nature and context of the activity and whether further investigation is required.

The school will not assume that an alert automatically demonstrates wrongdoing. Equally, repeated searches, attempts to bypass filtering or patterns of concerning activity will be taken seriously and considered within the wider safeguarding context.

8. Use of Devices and Technology in School

Technology is used to support teaching, learning, communication and school administration. Its use must always be appropriate, purposeful and consistent with the school's safeguarding expectations.

8.1 School Devices

Pupils and staff must use school devices responsibly and in accordance with the relevant Acceptable Use Agreements.

School devices must:

- Be used for authorised educational or professional purposes.
- Be accessed using individual school-approved accounts.
- Be used under appropriate staff supervision.
- Not be used to access, download or share inappropriate material.
- Not have unapproved software, applications or extensions installed.
- Not be used to bypass filtering or security arrangements.

Staff must ensure that devices are stored securely and that any loss, damage, suspected compromise or security concern is reported promptly.

Sensitive school information must only be stored or accessed through authorised, secure systems.

8.2 Approved Online Learning Platforms and Programmes

St John Fisher uses a range of approved digital platforms and programmes to support teaching and learning. These include:

- Google Classroom: used to support the organisation and sharing of learning resources and activities.

- IXL: used to provide pupils with opportunities to practise and develop their skills through interactive learning activities.
- Maths.co.uk: used to support mathematics learning, practice and assessment.
- SPaG.co.uk: used to support the development and assessment of spelling, punctuation and grammar.
- Kapow Primary: used to support the delivery of the school's curriculum through its digital teaching resources and materials.

The school also uses Little Wandle Letters and Sounds Revised and NELI (Nuffield Early Language Intervention) to support the development of pupils' early reading, phonics, language and communication skills. These are staff-led programmes and resources, used by teachers and teaching assistants to plan, deliver and support learning. They are not treated as pupil-facing online learning platforms in the same way as the services listed above.

The school may use additional digital resources where these have been approved for educational purposes.

All online platforms and programmes must be used appropriately and in accordance with the school's safeguarding and data protection requirements.

Staff must ensure that:

- Pupils access online platforms using school-issued accounts and credentials where applicable.
- Appropriate supervision is provided.
- Communication features, including chat, comments and shared documents, are disabled or restricted where possible and appropriate.
- Any communication or collaboration features that are enabled are appropriately managed and monitored by staff.
- Pupils do not share personal information or communicate independently with unknown users.
- Any concerns arising from the use of a platform are reported to the DSL.
-

The school will assess the suitability of online platforms before introducing them, taking account of safeguarding, data protection, age suitability and the information children may be required to provide.

8.3 Artificial Intelligence

The school recognises that artificial intelligence is becoming increasingly accessible and may offer opportunities to support teaching, learning and school administration. However, its use must be carefully considered and appropriately managed.

Staff must only use AI tools that have been approved by the school for the intended purpose.

Staff must not:

- Enter identifiable pupil, parent or staff information into unapproved AI tools.
- Upload photographs, videos, safeguarding records or confidential school documents into public AI systems.
- Rely on AI-generated information without checking its accuracy and suitability.
- Use AI in ways that compromise professional judgement, confidentiality or safeguarding.

Pupils must not independently access or use AI tools through school devices unless specifically authorised and supervised by a member of staff.

Any use of AI with pupils must be age-appropriate, educationally justified and subject to appropriate safeguarding and data protection arrangements.

The school will review its approach as AI technology develops.

9. Mobile Phones, Smart Devices and Personal Technology

9.1 Pupil Mobile Phones

At St John Fisher, we recognise that some parents may wish their child to carry a mobile phone when travelling to and from school.

Pupils may bring a mobile phone to school solely for travel safety. The following arrangements apply:

- Phones must be switched off before pupils enter the school site.
- On arrival at school, pupils must hand their phones directly to their class teacher.
- The class teacher is responsible for ensuring that phones handed in are securely locked away for the duration of the school day.

- Phones must remain switched off and must not be accessed by pupils during the school day.
- Phones will be returned to pupils by the class teacher at the end of the school day.
- Pupils must not use their phones to make calls, send messages, take photographs, record videos or access the internet during the school day.

If a pupil fails to hand in their phone, or is found using or accessing a phone during the school day, it will be taken from them and secured in the school office. A parent or authorised adult will be required to collect the phone.

Any misuse of a mobile phone that involves bullying, inappropriate images, safeguarding concerns or the sharing of harmful content will be dealt with in accordance with the relevant school policies and safeguarding procedures.

9.2 Other Personal Devices

Pupils must not bring personal tablets, smartwatches, cameras, gaming devices or other internet-enabled technology into school unless the Headteacher has given specific permission.

Any approved device must be used in accordance with the conditions set by the school.

9.3 Staff Personal Devices

Staff must maintain clear professional boundaries when using personal technology. Personal mobile phones and other personal devices must be kept out of sight and not used in classrooms or other areas where pupils are present, unless the Headteacher has given specific permission for an appropriate purpose.

Staff must not:

- Use personal devices to photograph, film or record pupils.
- Use personal messaging accounts or social media to communicate with pupils or parents.
- Share personal contact details with pupils.
- Use personal devices to access or store confidential pupil information.
- Use devices in a way that compromises the supervision or safety of children.

Where an exceptional circumstance requires the use of a personal device for an authorised school purpose, permission must be obtained from the Headteacher.

Staff must not allow personal device use to distract them from their responsibility to supervise and safeguard pupils.

9.4 Visitors and Volunteers

Visitors and volunteers are expected to respect the school's arrangements for mobile phones and personal devices.

They must not photograph, film or record pupils unless this has been specifically authorised by the school.

10. Staff Conduct and Online Communication

All staff are expected to maintain high standards of professional conduct, both in and outside school.

The same principles of respect, integrity and appropriate behaviour that apply in face-to-face relationships must also apply online.

Staff must:

- Use school-approved communication systems when contacting parents or carers.
- Use their school email account for professional correspondence.
- Maintain appropriate professional boundaries at all times.
- Ensure that communications are courteous, appropriate and capable of being shared with the Headteacher or other relevant professional if necessary.
- Protect confidential information and personal data.
- Seek advice if they are unsure whether an online interaction or communication is appropriate.

Staff must not:

- Communicate with pupils through personal email addresses, social media accounts or messaging services.
- Accept friend or follow requests from current pupils or engage with them through personal social media.

- Share information about pupils, families, colleagues or school matters on personal social media.
- Publish comments or images that could bring the school into disrepute or undermine professional trust.
- Use online communication to discuss confidential school matters.

Staff should be mindful that online activity can be permanent and may affect their professional reputation and the trust placed in them by pupils, parents and colleagues.

Any concern about inappropriate online contact or conduct involving a member of staff must be reported in accordance with the Child Protection and Safeguarding Policy and Staff Code of Conduct.

11. Social Media and Published Content

The school recognises that social media and online communication provide opportunities to celebrate achievements, share information and strengthen relationships with families.

However, the use of these platforms must be carefully managed to protect children, families and staff.

11.1 School Social Media and Website

Any content published through the school's website or official social media accounts must be authorised and appropriate.
The school will:

- Obtain and maintain appropriate parental permissions for the use of pupil photographs and videos.
- Respect parental decisions where permission has not been given.
- Avoid publishing children's full names alongside photographs or other identifying information.
- Ensure that published content reflects the school's Catholic ethos and professional standards.
- Take care not to disclose confidential or sensitive information.
- Ensure that images and information are shared only through approved school channels.

11.2 Parents and Carers

Parents and carers are asked to respect the privacy of all children and families when taking photographs or videos at school events.

They must not publish photographs or recordings containing other people's children on social media without the appropriate permission.

Parents should not use social media to discuss individual pupils, staff or safeguarding concerns. Any concerns should be raised directly with the school through the appropriate channels.

12. Online Safety Incidents and Safeguarding Responses

The school takes all online safety concerns seriously. An incident may involve a pupil, member of staff, parent, visitor or another person within the wider community.

Concerns may arise through a child's disclosure, staff observation, parental report, monitoring alerts or information received from an external agency.

All staff must report online safety concerns to the DSL or a DDSL without delay. Where a concern relates to the DSL, the alternative safeguarding reporting arrangements in the Child Protection and Safeguarding Policy must be followed.

12.1 Recording and Reporting

Safeguarding concerns arising from online activity must be recorded on CPOMS in accordance with the school's safeguarding procedures.

Records should include:

- The nature of the concern and how it came to light.
- The child's own words where a disclosure has been made.
- Relevant dates, times and details of the incident.
- Any immediate action taken to protect the child.
- Decisions made and the reasons for those decisions.
- Referrals, communications and subsequent actions.

Staff must record facts accurately and avoid making assumptions or conducting their own investigations.

12.2 Responding to a Pupil Disclosure

If a child reports an online safety concern, staff must:

- Listen carefully and remain calm.
- Reassure the child that they have done the right thing by speaking to an adult.
- Avoid asking leading questions or pressing the child for unnecessary detail.
- Never promise confidentiality.
- Explain that information may need to be shared with people who can help keep them safe.
- Report the concern to the DSL or DDSL immediately.
- Record the disclosure in accordance with safeguarding procedures.

12.3 Inappropriate or Harmful Content

If a pupil accesses inappropriate or harmful material, the school will consider the nature of the content, how it was accessed and whether there are any wider safeguarding concerns.

The school will:

- Take immediate steps to protect the child and prevent further exposure.
- Notify the DSL where the material raises a safeguarding concern.
- Record the incident and actions taken.
- Inform parents where appropriate.
- Consider whether additional support, education or external advice is required.
- Review whether the incident identifies a weakness in filtering, supervision or school procedures.

Where criminal activity is suspected, the school will seek advice from the appropriate external agencies.

12.4 Cyberbullying and Online Harassment

Cyberbullying will be dealt with in accordance with the Anti-Bullying Policy and Behaviour Policy.

The school will consider:

- The nature and seriousness of the behaviour.
- Whether the behaviour is repeated or targeted.
- The impact on the child or children involved.

- Whether discriminatory, threatening or abusive behaviour has occurred.
- Whether there are wider safeguarding concerns.

Incidents occurring outside school may still require a school response where they affect pupils' safety, welfare, relationships or ability to feel safe in school.

12.5 Sharing of Nudes and Semi-Nudes

The school recognises that children may be pressured, manipulated or coerced into creating or sharing nude or semi-nude images. This is a safeguarding concern and must never be treated simply as a matter of poor behaviour.

Any incident involving the creation, possession or sharing of nude or semi-nude images must be reported to the DSL immediately.

The school will follow the latest UKCIS guidance and the procedures set out in Keeping Children Safe in Education.

Staff must not:

- View, download, copy, print or forward an image.
- Ask a child to send or show an image.
- Investigate the incident independently.
- Delete or interfere with potential evidence.

The DSL will assess the circumstances, consider the immediate safety and welfare of the child, seek advice from the police or children's social care where appropriate and ensure that parents are involved where it is safe and appropriate to do so.

The child's welfare and protection will remain the priority throughout.

12.6 Online Grooming, Exploitation and Radicalisation

Where there are concerns that a child is being groomed, exploited, threatened, coerced or exposed to extremist or radicalising material, the school will follow its Child Protection and Safeguarding Policy and make appropriate referrals.

The DSL will consider whether the concern requires referral to children's social care, the police, the Local Authority Prevent team or other relevant agencies.

Where a child may be at immediate risk of harm, urgent action will be taken.

12.7 Allegations and Concerns Involving Staff

Any concern that a member of staff, volunteer or other adult has behaved inappropriately online or used technology in a way that may place a child at risk must be reported immediately in accordance with the school's safeguarding procedures.

Where the concern meets the threshold for an allegation, the Headteacher will follow the appropriate Local Authority Designated Officer (LADO) procedures.

Where a concern relates to the Headteacher, it must be reported to the Chair of Governors in accordance with the Child Protection and Safeguarding Policy.

13. Data Protection, Privacy and Information Security

The school has a responsibility to protect the personal information of pupils, parents, staff and other members of the school community.

All staff must comply with the school's Data Protection Policy and ensure that personal information is handled securely and appropriately.

Staff must:

- Access personal information only where there is a legitimate professional reason.
- Use approved school systems to store and share information.
- Keep passwords secure and never share individual login details.
- Lock devices when they are unattended.
- Take care when sending emails and check recipients before sharing information.
- Avoid sending sensitive information through unsecured communication channels.
- Report any suspected data breach, loss of information or unauthorised access immediately.

Pupil photographs, videos and other personal information must only be used and shared in accordance with the school's permissions and data protection arrangements.

The school will ensure that online platforms and digital services are assessed appropriately before use, including consideration of their data protection arrangements and the personal information they collect.

14. Remote Learning and Online Meetings

Where remote learning or online meetings are required, the school will use approved platforms and ensure that appropriate safeguarding arrangements are in place.

Staff must:

- Use school-approved accounts and communication systems.
- Ensure that online interactions are professional and appropriate.
- Follow the school's expectations regarding dress, setting and professional conduct.
- Avoid using personal messaging accounts to communicate with pupils.
- Ensure that any recorded content is authorised and stored securely.
- Consider the privacy and safeguarding implications of online meetings.

Pupils and parents will be given clear guidance about the appropriate use of online learning platforms and how to report any concerns.

15. Working in Partnership with Parents and Carers

We recognise that children's online experiences extend well beyond the school gates. Effective online safety therefore depends on a partnership between school and home.

The school will support parents and carers by:

- Sharing advice and guidance about emerging online risks.
- Signposting trusted resources, including CEOP Education, Childnet and Internet Matters.
- Providing information about parental controls, age restrictions and safe device use.
- Raising awareness of online risks through newsletters, meetings and other appropriate communication.
- Working with families when concerns arise about a child's online safety.

Parents are encouraged to speak to the school if they are worried about their child's online experiences, particularly where there may be bullying, inappropriate contact, exploitation or exposure to harmful material.

We recognise that families may have different levels of confidence and experience when it comes to technology. Our approach will be supportive and focused on helping parents develop the knowledge they need to protect their children.

16. Staff Training and Awareness

All staff must understand that online safety is part of their safeguarding responsibilities.

Online safety will form part of the school's safeguarding training and updates. Staff will be made aware of emerging risks, changes in technology and any changes to the school's procedures.

Training and guidance will ensure that staff understand:

- The range of online risks children may encounter.
- How to recognise signs of online abuse, grooming and exploitation.
- How to respond to disclosures.
- How to report and record concerns.
- The school's filtering and monitoring arrangements.
- The appropriate use of school technology and online platforms.
- Their responsibilities regarding confidentiality, professional conduct and data protection.

Staff will be expected to seek advice from the DSL or Headteacher if they are uncertain about any aspect of online safety.

17. Monitoring, Evaluation and Policy Review

The effectiveness of this policy will be monitored through the school's safeguarding arrangements and regular review of online safety practice.

The Headteacher and DSL will consider:

- The nature and frequency of online safety incidents.
- Patterns or repeated concerns recorded on CPOMS.

- The effectiveness of filtering and monitoring.
- Staff understanding and compliance with the policy.
- The effectiveness of online safety teaching.
- Feedback from pupils, parents and staff.
- Changes in technology and emerging online risks.
- Any changes to statutory guidance or relevant legislation.

Significant concerns and developments will be reported to the Governing Body through the appropriate safeguarding and governance arrangements.

This policy will be reviewed annually, or sooner where changes in legislation, statutory guidance, technology or safeguarding practice make an earlier review necessary.

The Governing Body will approve the policy and ensure that it remains effective in protecting the children and wider community of St John Fisher Catholic Primary School.

APPENDIX 1: PUPIL ACCEPTABLE USE AGREEMENT



PUPIL ACCEPTABLE USE AGREEMENT

Using technology safely and responsibly

At St John Fisher, we use technology to help us learn, explore, create and communicate. We want everyone to enjoy using technology safely and responsibly.

Our Catholic mission and LIGHT values - Love, Integrity, Growth, Hope and Togetherness - guide the way we behave, both online and offline.

When I use a computer, tablet or other digital device in school, I agree to follow these expectations.

My responsibilities

I will be kind and respectful.

- I will use kind and respectful language when using technology.
- I will treat others as I would like to be treated.
- I will not send, write or share unkind, threatening or hurtful messages.
- I will not use technology to upset, embarrass or bully anyone.
- I will respect other people's work, photographs and personal information.

I will keep myself safe.

- I will only use websites, apps and programmes that my teacher has said I can use.
- I will not search for or deliberately access anything that is inappropriate or upsetting.
- I will keep my name, address, passwords, photographs and other personal information private.
- I will never share my password with another pupil.
- I will not communicate online with people I do not know.

- I will tell an adult if someone online makes me feel uncomfortable, asks me for personal information or wants me to keep a secret.

I will make sensible choices.

- I will use technology for the learning activity my teacher has given me.
- I will follow instructions and use devices carefully.
- I will not change settings, download programmes or install apps without permission.
- I will not use another person's account or pretend to be someone else.
- I will not take or share photographs, videos or recordings of others without permission.
- I will not copy someone else's work and pretend it is my own.
- I will not use artificial intelligence tools unless my teacher has given me permission.

I will speak up if something goes wrong.

- I will tell my teacher or another trusted adult if I see something upsetting, inappropriate or worrying.
- I will tell an adult if someone sends me an unkind message or behaves inappropriately online.
- I will not hide a mistake or try to deal with a worrying situation on my own.
- I understand that I will not be in trouble for asking for help.

Using technology in school

I understand that:

- My use of school technology and online platforms may be filtered and monitored to help keep everyone safe.
- I must use my school account responsibly and keep my login details secure.
- I must only access learning platforms and resources approved by my teacher.
- I must look after school devices and report any damage or problems.
- I must follow my teacher's instructions when using technology.

Mobile phones and personal devices

I understand that:

- If I bring a mobile phone to school, it is only for safety when travelling to and from school.
- I must hand my phone to my class teacher when I arrive at school.
- My phone will be securely locked away throughout the school day.

- My phone will be returned to me at the end of the school day.
- I must not use my phone or another personal device during the school day.
- I must not bring other personal internet-enabled devices into school unless I have permission.

If I do not follow the agreement

I understand that if I do not follow these expectations, a member of staff will speak to me about my choices. The school may restrict my access to technology and take further action in line with its Behaviour Policy and Online Safety Policy.

I understand that these rules help to protect me and everyone in our school community.

Our promise

We will use technology with kindness, honesty and responsibility, remembering that our words and actions matter, both online and offline.

Pupil agreement

I have read and understood this agreement. I will do my best to follow these expectations whenever I use technology in school.

Pupil name: _____ Year: _____

Pupil signature: _____ Date: _____

Parent/carer acknowledgement

I have read this agreement with my child and understand the school's expectations for the safe and responsible use of technology.

I will support my child in following these expectations and encourage them to speak to a trusted adult if they experience anything online that causes concern.

Parent name: _____ Year: _____

Parent signature: _____ Date: _____