St Bernard's RC Primary & Nursery School



Online Safety and Acceptable Use Policy

(including use of mobile phones and devices)

Approved by Governors: Autumn 2026

Review Date: Autumn 2028

Contents

1. Aims

2. Legislation and Guidance

3. Roles and Responsibilities

4. Educating Children About Online Safety

5. Educating Parents and Carers About Online Safety

6. Cyber-Bullying

7. Acceptable Use of the Internet and Technology in School

8. Mobile Phones and Personal Devices

9. Staff Use of Technology and Work Devices

10. Responding to Online Safety Incidents and Misuse

11. Training

12. Monitoring and Review

13. Links with Other Policies

Appendix 1: Staff, Governors, Volunteers and Visitors Acceptable Use Agreement
Appendix 2: Online Safety Staff Training Self-Audit

1. Aims

At St Bernards RC Primary and Nursery School, we recognise that technology plays an important role in children's learning, communication and everyday lives. We are committed to ensuring that all members of our school community can use technology safely, responsibly and respectfully.

Our approach to online safety is part of our wider safeguarding responsibilities and reflects our Catholic ethos, including our commitment to respect, dignity, kindness and the wellbeing of every child.

This policy aims to:

- Protect children, staff, governors, volunteers and visitors from online risks and harm.
- Provide a safe and secure environment in which technology can support learning.
- Teach children how to use technology safely, responsibly and respectfully.
- Help children recognise online risks and know how and when to seek help.
- Support parents and carers in understanding the risks children may encounter online.
- Ensure staff understand their responsibilities regarding online safety.
- Provide clear procedures for reporting, recording and responding to online safety concerns.
- Ensure that appropriate filtering and monitoring systems are in place.
- Promote positive online behaviour and relationships.
- Embed online safety throughout the curriculum and wider safeguarding provision.

The four key categories of online risk

Our approach to online safety considers four main areas of risk:

Content - children may encounter inappropriate, illegal or harmful material, including violent, sexual, discriminatory, extremist or otherwise unsuitable content.

Contact - children may experience harmful interactions with others online, including bullying, peer pressure, grooming, exploitation or contact from people they do not know.

Conduct - children may behave online in ways that put themselves or others at risk of harm, including bullying, sharing inappropriate material or personal information, or making and sharing images without appropriate consent.

Commerce - children may be exposed to financial scams, phishing, inappropriate advertising, online gambling or pressure to purchase goods or services. We recognise that these risks can overlap and that children may be particularly vulnerable because of their age, additional needs, circumstances or previous experiences.

2. Legislation and Guidance

This policy should be read alongside current statutory guidance and legislation relating to safeguarding, education and online safety.

It reflects, where applicable, the principles and requirements contained within:

- The Department for Education's Keeping Children Safe in Education.
- Department for Education guidance on Teaching Online Safety in Schools.
- Department for Education guidance on Preventing and Tackling Bullying, including cyber-bullying. Department for Education guidance on Searching, Screening and Confiscation.
- Department for Education guidance relating to Mobile Phones in Schools.
- Department for Education guidance relating to relationships, health and sex education.
- UK Council for Internet Safety guidance.
- Relevant guidance concerning the sharing of nude and semi-nude images.
- The Education Act 1996.
- The Education and Inspections Act 2006.
- The Equality Act 2010.
- The Education Act 2011.
- The UK GDPR and Data Protection Act 2018.
- Relevant Prevent and safeguarding guidance.
- The National Curriculum programmes of study for Computing.

This policy will be reviewed regularly to ensure that it reflects changes in legislation, statutory guidance, technology and emerging online risks.

3. Roles and Responsibilities

3.1 The Governing Board

The Governing Board has overall responsibility for ensuring that appropriate arrangements are in place to safeguard children online.

Governors will:

- Ensure that they understand this policy and their safeguarding responsibilities.
- Monitor the effectiveness of the school's online safety arrangements.
- Ensure that online safety is appropriately considered within the school's wider safeguarding arrangements.
- Receive appropriate information regarding online safety incidents and trends.
- Ensure that online safety provision considers the needs of vulnerable children and children with SEND.
- Support the school in ensuring that appropriate filtering and monitoring arrangements are in place.

- Ensure that staff and governors receive appropriate safeguarding and online safety training.
- Governors will maintain an awareness that online safety is a rapidly changing area and that policies and procedures must be reviewed accordingly.

3.2 The Headteacher

The Headteacher is responsible for:

- Ensuring that this policy is implemented consistently.
- Ensuring that staff understand their responsibilities.
- Working with the Safeguarding team and Computing Lead to ensure effective online safety arrangements. Ensuring that concerns are dealt with appropriately.
- Ensuring that appropriate training is provided.
- Working with the Governing Board to monitor and review online safety provision.
- Ensuring that serious incidents are escalated to the appropriate external agencies where necessary.

3.3 Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety as part of their wider safeguarding role. The DSL will:

- Work with the Headteacher and staff to implement this policy.
- Respond to online safety concerns in accordance with the school's safeguarding procedures.
- Ensure that online safety incidents are appropriately recorded.
- Ensure that concerns involving online abuse, exploitation, grooming or harmful behaviour are appropriately assessed.
- Liaise with parents and carers where appropriate.
- Liaise with external agencies, including the police and children's social care, where necessary.
- Ensure that online safety concerns are considered within the school's safeguarding systems.
- Monitor patterns and trends in online safety incidents.
- Ensure that staff receive appropriate online safety training.
- Provide advice and support to staff when online safety concerns arise.
- The DSL will ensure that safeguarding concerns are managed in accordance with the school's Child Protection and Safeguarding Policy.

3.4 Computing Lead

The Computing Lead, working with the Headteacher and relevant technical support, will:

- Support the development of children's digital literacy and online safety knowledge.
- Ensure online safety is appropriately incorporated into the Computing curriculum.
- Support staff in using technology safely and effectively.
- Work with the school's IT provider to ensure appropriate technical

safeguards are in place.

- Support the effective use of filtering and monitoring systems.
- Report concerns regarding technology, filtering or monitoring to the Headteacher and/or DSL.
- Support the school in responding to technical online safety incidents.
-

3.5 All Staff and Volunteers

All staff and volunteers have a responsibility to safeguard children when using technology. Staff and volunteers will:

- Read and follow this policy.
- Follow the school's Acceptable Use Agreement.
- Model appropriate, respectful and responsible online behaviour.
- Ensure children use technology appropriately and safely.
- Report online safety concerns promptly to the DSL.
- Never knowingly access, share or distribute inappropriate material using school systems. Maintain professional boundaries when communicating electronically.
- Protect passwords and confidential information.
- Follow the school's data protection and information security requirements. Report lost or stolen devices promptly. Respond appropriately to concerns raised by children about online activity.
- Staff should maintain an attitude of "it could happen here" when considering online safeguarding concerns.

3.6 Parents and Carers

Parents and carers play an important role in supporting children's online safety. Parents and carers are expected to:

- Support the school's online safety expectations.
- Talk regularly with their children about safe and responsible technology use.
- Encourage children to report anything online that worries or upsets them.
- Notify the school of concerns that may affect their child's wellbeing or safety.
- Support their child in following the school's Acceptable Use Agreement.
- Familiarise themselves with the school's online safety guidance.
- Parents and carers are encouraged to seek advice from recognised online safety organisations and to contact the school if they have concerns.
-

3.7 Visitors and Members of the Community

Visitors, volunteers and members of the community who are permitted to use the school's technology or internet facilities will be expected to comply with the school's Acceptable Use Agreement. Use of school technology must be appropriate, lawful and consistent with safeguarding, confidentiality and data protection requirements.

4. Educating Children About Online Safety

Online safety is an integral part of the curriculum at St Bernards RC Primary and Nursery Children will be taught how to:

- Use technology safely and responsibly.
- Treat others with kindness and respect online.
- Recognise appropriate and inappropriate online behaviour.
- Keep personal information private.
- Create and protect appropriate passwords.
- Recognise that people online may not always be who they claim to be.
- Understand the importance of speaking to a trusted adult if something worries them.
- Identify inappropriate, harmful or upsetting content.
- Report concerns about online content or contact.
- Understand the potential consequences of online behaviour.
- Understand the importance of consent, privacy and respect when sharing information or images. Develop an appropriate level of critical thinking when accessing online information.
- Understand that information shared online can be difficult to remove.

Online safety will be taught through Computing, Relationships and Health Education, PSHE/RSE, assemblies, worship and other curriculum opportunities where appropriate.

Early Years Foundation Stage

In Nursery and Reception, children will be supported to develop age-appropriate understanding of technology and safe use. Children will learn to:

- Use technology with adult support.
- Handle equipment safely.
- Understand that some things should only be accessed with an adult.
- Tell a trusted adult if something makes them feel worried or uncomfortable.
- Begin to understand the importance of kindness and respectful behaviour when using technology. Key Stage 1

Children will learn to: Use technology safely and respectfully; Keep personal information private; Understand that not everything online is suitable or true; Identify trusted adults who can help them; Report anything that makes them feel worried, uncomfortable or unsafe.

Key Stage 2

Children will develop their understanding of: Online identity and reputation; Privacy and personal information; Online relationships and communication; Cyber-bullying; Online grooming and inappropriate contact; Harmful or misleading content; Sharing photographs and videos; Password security; Online scams and financial risks; The permanence of online activity; How to report concerns and seek support.

Teaching will be adapted where necessary to meet the needs of vulnerable children and

children with SEND.

5. Educating Parents and Carers About Online Safety

The school recognises the importance of working in partnership with parents and carers. Online safety information may be shared through: The school website, Newsletters, Parent information sessions, Parents' evenings, Letters and communications home, Assemblies and curriculum activities, and signposting to recognised online safety organisations.

Parents and carers will be informed about how technology is used within school and, where appropriate, the filtering and monitoring systems used to help protect children. Parents should contact the Headteacher or DSL if they have concerns regarding online safety.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying is bullying that takes place using digital technology, including mobile phones, messaging services, social media, online games and other digital platforms. Cyber-bullying may include:

- Sending threatening or abusive messages.
- Deliberately excluding someone from online groups.
- Sharing embarrassing photographs or videos.
- Spreading rumours online.
- Creating fake accounts.
- Posting hurtful or discriminatory comments.
- Sharing personal information without permission.
- Encouraging others to target an individual.

Cyber-bullying can occur both within and outside school and may have a significant impact on a child's emotional wellbeing and sense of safety.

6.2 Preventing and Responding to Cyber-Bullying

The school will:

- Teach children about respectful online behaviour.
- Explain what cyber-bullying is and how to report it.
- Encourage children to speak to a trusted adult.
- Provide support to children who experience cyber-bullying.
- Address cyber-bullying in accordance with the Behaviour Policy.
- Work with parents and carers where appropriate.
- Consider whether external agencies need to be involved.
- Record significant incidents appropriately.

Where online behaviour amounts to a safeguarding concern or may constitute a criminal

offence, the DSL will consider whether the matter should be referred to the police or another appropriate agency.

6.3 Cyber-Bullying responsibilities

Primary responsibility for monitoring out-of-school device use rests with parents and carers. However, the school reserves the right to investigate and sanction incidents of out-of-school online bullying or inappropriate app use where the conduct:

Impacts the safety, well-being, or learning environment of pupils while at school;
Involves severe peer-on-peer abuse or harassment targeting members of the school community; or undermines the orderly running and discipline of the school.

For incidents falling outside school jurisdiction, the school will direct families to appropriate external reporting channels (such as the police, CEOP, or app providers) and offer pastoral support to affected pupils.

6.4 Searching Electronic Devices

The school may search or confiscate electronic devices where authorised staff have reasonable grounds to believe that the device: Poses a risk to staff or children; Contains evidence of a breach of school rules; Contains evidence relating to an offence; Has been used to cause harm or disrupt the safe running of the school.

Any search will be undertaken in accordance with current Department for Education guidance, the school's Behaviour Policy and safeguarding procedures. If staff believe a device may contain an indecent image of a child, staff must not intentionally view the image. The device should be secured and the matter reported immediately to the DSL, who will determine the appropriate safeguarding response. Any material that may constitute evidence of an offence must not be deleted.

7. Acceptable Use of the Internet and Technology in School

Technology provided by the school is primarily for educational purposes and for carrying out legitimate school duties. All users must:

- Use school technology responsibly.
- Follow the school's Acceptable Use Agreement.
- Respect other people's privacy.
- Keep passwords secure.
- Report inappropriate content or contact immediately.
- Follow instructions from staff.
- Use school systems only for appropriate purposes.
- Respect copyright and intellectual property.
- Take care of school equipment.

The school uses filtering and monitoring systems to help protect children and staff from inappropriate online content. Users should not attempt to bypass or disable filtering or security

systems. Further expectations are set out in the Acceptable Use Agreements contained within the appendices.

8. Mobile Phones and Personal Devices

St Bernards RC Primary and Nursery School is a 'Smartphone-free school'. Therefore, it does not encourage children to bring smartphones, smartwatches or any other internet-enabled personal devices into school. Where a child genuinely needs a mobile phone because they travel to or from school independently, a simple, non-smart device, a 'brick phone' without internet connectivity, is recommended. Pupils may only bring these devices into school with express permission from the headteacher for the purpose of emergency contact when walking home alone. Phones will be safely stored at the front office and will be given to the children at the ned of the school day.

Any breach of these expectations may result in the device being confiscated and/or other appropriate action being taken in accordance with the Behaviour Policy.

9. Staff Use of Technology and Work Devices

Staff are expected to use technology professionally, responsibly and securely. When using school devices or accessing school systems, staff must:

- Keep devices password-protected.
- Use strong passwords and keep them confidential.
- Lock devices when unattended.
- Keep software and operating systems updated.
- Use appropriate security and antivirus measures where required.
- Never allow unauthorised people to use school devices.
- Protect confidential school and pupil information.
- Follow the school's Data Protection and Information Security Policies.
- Report lost or stolen devices immediately.
- Only access information necessary for their role.
- Avoid using personal email or messaging accounts for confidential school business.
- Maintain appropriate professional boundaries when communicating with pupils and families.

Work devices should not normally be shared with family members or friends. Staff must not use school devices or systems to access, create, store or share inappropriate material. Any concerns about the security of a school device should be reported to the Headteacher or appropriate IT support immediately.

10. Responding to Online Safety Incidents and Misuse

The school will respond to online safety incidents promptly and proportionately. Where a child misuses technology or the internet, the school will consider: The nature and seriousness of the incident; The child's age and level of understanding; Whether anyone has been harmed or placed at risk; Whether the behaviour represents a safeguarding concern; Whether parents/carers should be informed; Whether the Behaviour Policy applies; Whether external agencies should be contacted.

Where a staff member misuses technology or school systems, the matter will be dealt with in accordance with the Staff Code of Conduct and relevant disciplinary procedures. Serious incidents involving illegal activity, significant safeguarding concerns or potential criminal offences will be referred to the appropriate external agency where necessary. All safeguarding concerns will be managed in accordance with the school's Child Protection and Safeguarding Policy.

11. Training

Online safety training forms part of the school's wider safeguarding training. All new staff will receive appropriate online safety information as part of their induction. Staff will receive regular safeguarding and online safety updates, including information about emerging risks.

Training will cover areas including:

- Online abuse and exploitation.
- Cyber-bullying.
- Online grooming.
- Harmful online content.
- Appropriate professional use of technology.
- Data protection and confidentiality.
- Online radicalisation and extremism.
- Sharing of nude and semi-nude images.
- Peer-on-peer abuse.
- Reporting and responding to online safety concerns.
- Appropriate use of artificial intelligence and emerging technologies where relevant.

The DSL and Deputy DSLs will undertake safeguarding training, including online safety, in accordance with current statutory requirements and will maintain up-to-date knowledge. Governors and volunteers will receive appropriate safeguarding and online safety information according to their roles.

12. Monitoring and Review

Online safety concerns will be recorded using the school's safeguarding and recording system, CPOMS. The DSL will monitor online safety incidents to identify patterns, trends or emerging risks. The school will monitor the effectiveness of its filtering and monitoring arrangements and respond promptly to identified weaknesses.

This policy will be reviewed annually, or sooner where there are significant changes to legislation, guidance, technology or identified risks. The policy will be reviewed by the Headteacher, DSL and Computing Lead and presented to the Governing Board for approval.

The annual review will consider: Online safety incidents; Safeguarding concerns; Feedback from children, staff and parents; Staff training needs; Filtering and monitoring arrangements; Emerging online risks; Changes to statutory guidance.

13. Links with Other Policies

This policy should be read alongside the school's:

- Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Staff Disciplinary Procedures
- Data Protection Policy
- Privacy Notices
- Information Security Policy
- Behaviour Policy
- Data Breach Policy
- Complaints Policy
- Computing Policy
- Relationships and Health Education / RSE Policy
- Special Educational Needs and Disabilities Policy
- Acceptable Use Agreements

Appendix 1: Staff, Governors, Volunteers and Visitors Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor: _____

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and

systems.

I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care

do so too.

Signed: _____ Date: _____

Appendix 2: Online Safety Staff Training Self-Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No or Comments
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you aware of the ways pupils can abuse their peers online?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	