

St. Bede's Catholic Primary School

E-Safety Policy



Approval and Review

Approved by Governing Body – (To be ratified by governors in November 2026)

Online Safety Lead – Mrs K. McVittie

Designated Safeguarding Lead (DSL) Mrs C. Devine

Review Frequency - Annually

Next Review Date – June 2027

Related Policies – BCCET Acceptable Use Policy, BCCET AI Guidance Policy, Keeping Children Safe in Education.

1. Introduction

At St. Bede's Catholic Primary School, we recognise that technology plays an essential role in education, communication and daily life. We are committed to creating a culture where pupils, staff, governors and parents can benefit from technology safely, responsibly and positively.

Online safety is a safeguarding issue and forms an integral part of our wider safeguarding responsibilities. The school aims to equip pupils with the knowledge, skills and resilience required to stay safe online both within and beyond school.

This policy applies to all members of the school community, including:

Pupils
Staff
Governors
Volunteers
Contractors
Visitors
Parents and carers

This policy should be read alongside all safeguarding, data protection and information security policies adopted by Bishop Chadwick Catholic Education Trust (BCCET).

2. Aims

The aims of this policy are to:

Safeguard and promote the welfare of children through effective online safety practice.
Protect staff and pupils from online risks.
Promote safe and responsible use of technology.
Ensure compliance with statutory safeguarding requirements.
Support the effective use of technology to enhance teaching and learning.
Promote digital citizenship and responsible online behaviour.
Protect personal and sensitive information.
Ensure appropriate filtering and monitoring arrangements are in place.

3. Legislative Framework

This policy is informed by:

Keeping Children Safe in Education (KCSIE) 2025	The Equality Act 2010
Working Together to Safeguard Children	Prevent Duty Guidance
The Education Act 2002	ICO Guidance on Artificial Intelligence and Data Protection
The Data Protection Act 2018	DfE Guidance on Generative Artificial Intelligence in Education
UK GDPR	

The Online Safety Act 2023
The Computer Misuse Act 1990
The Communications Act 2003
The Malicious Communications Act 1988

Bishop Chadwick Catholic Education Trust
Acceptable Use Policy
Bishop Chadwick Catholic Education Trust Artificial
Intelligence Guidance Policy

4. Online Safety and Safeguarding

The school recognises that online safety is a fundamental aspect of safeguarding.

Online risks are categorised into four areas:

Content

Exposure to harmful, illegal or inappropriate content, including:

- Pornography
- Extremist material
- Hate content
- Self-harm and suicide-related content
- Violence
- Misinformation and disinformation

Contact

Harmful interactions with others online, including:

- Grooming
- Sexual exploitation
- Radicalisation
- Harassment
- Coercion

Conduct

Behaviour that increases risk online, including:

- Cyberbullying
- Sharing personal information
- Sending inappropriate images
- Peer-on-peer abuse
- Misuse of technology

Commerce

Risks associated with online transactions, including:

- Fraud
- Scams
- Gambling
- Financial exploitation
- Phishing attacks

Any concerns regarding online safety will be managed in accordance with the school's Child Protection and Safeguarding Policy.

5. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure online safety is effectively embedded within safeguarding arrangements.
- Monitor implementation of this policy.
- Ensure appropriate filtering and monitoring systems are in place.
- Receive updates regarding online safety incidents and developments.

Headteacher

The Headteacher will:

- Lead the implementation of this policy.
- Ensure appropriate staff training is provided.
- Ensure online safety concerns are addressed appropriately.
- Work with the DSL and Trust teams to monitor compliance.

Designated Safeguarding Lead (DSL)

The DSL will:

- Lead on safeguarding aspects of online safety.
 - Record and respond to online safety concerns.
 - Liaise with external agencies where necessary.
 - Monitor trends and emerging risks.
- Computing / Online Safety Lead

The Online Safety Lead will:

- Coordinate online safety education.
- Review filtering and monitoring arrangements.
- Support staff training.
- Keep abreast of national guidance and emerging technologies.

Staff

All staff must:

- Read and follow this policy.
- Maintain professional conduct online.
- Report concerns immediately.
- Model safe and responsible technology use.
- Undertake regular training.

Pupils

Pupils are expected to:

- Follow school acceptable use expectations.
- Use technology safely and responsibly.

Report concerns to a trusted adult.
Respect others online.

6. Online Safety Education

Online safety education is embedded throughout the curriculum.

Pupils will be taught:

- How to stay safe online.
- How to protect personal information.
- How to recognise scams and phishing.
- Safe use of social media.
- Responsible communication.
- Digital wellbeing.
- Cyberbullying awareness.
- Age-appropriate understanding of Artificial Intelligence.
- How to report concerns.

Online safety will be delivered through:

- Computing
- PSHE
- Assemblies
- Collective Worship where appropriate
- National events such as Safer Internet Day

7. Working with Parents and Carers

The school recognises the vital role parents and carers play in promoting online safety.

The school will provide information through:

- School newsletters
- Website updates
- Parent workshops
- Information leaflets
- Social media communications

Parents are encouraged to:

- Discuss online safety regularly at home.
- Monitor age-appropriate use of devices.
- Use parental controls where appropriate.
- Report concerns to school.

8. Artificial Intelligence (AI)

The school recognises the growing role of Artificial Intelligence (AI) within education.

AI tools may support:

- Teaching and learning
- Resource creation
- Administrative tasks
- Accessibility support

However, AI must never replace professional judgement.

Staff Responsibilities

Staff must:

- Critically evaluate AI-generated content.
- Check outputs for accuracy, bias and appropriateness.
- Ensure all content is suitable for pupils.
- Comply with Trust AI guidance.

Staff must not:

- Enter safeguarding information into unauthorised AI systems.
- Enter pupil names, addresses or identifying information into unauthorised AI tools.
- Upload confidential school information into unauthorised AI platforms.

Educational Use

Pupils will be taught:

- What AI is.
- Benefits and limitations of AI.
- How to critically evaluate AI-generated content.
- How to use AI responsibly and ethically.

Any new AI system processing personal data must be approved through Trust procedures and may require a Data Protection Impact Assessment (DPIA).

9. Filtering and Monitoring

The school employs appropriate filtering and monitoring systems through BCCET.

These systems aim to:

- Block illegal and inappropriate content.
- Reduce safeguarding risks.
- Detect concerning online activity.
- Support safe educational use of technology.

Filtering and monitoring arrangements are regularly reviewed by:

- Headteacher
- DSL
- Online Safety Lead
- BCCET ICT Team

Any safeguarding concerns identified through monitoring systems will be referred to the DSL.

10. Cyber Security

The school recognises the importance of protecting systems, devices and information.

All users must:

- Use strong passwords.
- Keep passwords confidential.
- Lock devices when unattended.
- Report suspicious emails.
- Report suspected breaches immediately.
- Use authorised software only.

Users should be alert to:

- Phishing emails
- Fake websites
- Social engineering attempts
- Suspicious links
- Malware and viruses

Cyber security incidents will be reported to the Headteacher and BCCET ICT Team.

11. Email and Digital Communication

Staff must only use approved school communication systems.

Communication with pupils and parents must:

- Be professional.
- Use official school systems.
- Be appropriate and transparent.

Staff must not:

- Use personal email accounts for school business.
- Communicate with pupils through personal messaging apps.
- Use personal social media accounts to communicate with pupils.

12. Social Media

The school recognises the positive role social media can play when used responsibly.

Official school accounts may be used to:

- Celebrate achievements.
- Share information.
- Communicate with families.

Staff must:

- Maintain professional boundaries.
- Protect confidential information.
- Follow Trust social media guidance.

Staff must not:

- Accept friend requests from current pupils.
- Communicate privately with pupils through social media.
- Post content that could bring the school or Trust into disrepute.

13. Mobile Devices**Pupils**

Pupils who bring mobile phones to school must hand them to a member of staff at the start of the day.

Devices will be securely stored and returned at the end of the day.

Pupils must not use mobile phones during the school day unless authorised by staff.

Smart watches capable of:

- Internet access
- Messaging
- Photography
- Video recording

must be switched off and handed in during the school day.

Staff

Staff mobile phones must:

- Be kept out of sight during teaching time.
- Not be used in teaching areas except for emergencies.
- Not be used to photograph pupils.

14. Photography and Video Recording

Only school-approved devices should be used to take photographs or videos of pupils.

Photographs and recordings must:

- Support legitimate educational purposes.
- Comply with parental consent arrangements.
- Be stored securely.
- Be transferred to approved storage promptly.

Staff must not use personal devices to take photographs, videos or audio recordings of pupils where their identity can be revealed.

Care must be taken to ensure photographs do not contain:

- Personal information
- Assessment data
- Computer screens displaying confidential information

15. Data Protection

All users must comply with:

- UK GDPR
- Data Protection Act 2018
- Trust Data Protection Policies

Personal data must:

- Be processed lawfully.
- Be stored securely.
- Be shared only when authorised.
- Be protected from loss, misuse or unauthorised access.

Data breaches must be reported immediately.

16. Reporting Concerns

All online safety concerns must be reported immediately.

Examples include:

- Cyberbullying
- Inappropriate content
- Suspicious communications
- Online grooming concerns
- Data breaches
- Misuse of technology
- AI-related concerns

Concerns should be reported to:

- Class Teacher
- DSL
- Headteacher
- Online Safety Lead

All concerns will be recorded and investigated appropriately.

17. Sanctions

Failure to comply with this policy may result in:

Pupils

- Restricted access to technology
- Behaviour sanctions
- Parent meetings
- Safeguarding intervention

Staff

- Withdrawal of access rights
- Management action
- Disciplinary procedures
- Referral to external agencies where appropriate

18. Monitoring and Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- New technologies emerge.
- Significant incidents occur.
- Updated Trust guidance is issued.

The Governing Body will receive regular updates regarding online safety arrangements and significant incidents.