

BRAMCOTE CHURCH OF ENGLAND PRIMARY SCHOOL



ONLINE SAFETY POLICY 2026–2027

Date Approved: Awaiting ratification by FGB October 2026

Review Cycle: Annual

Next Review: September 2027 (or earlier if legislation or guidance changes)

Approved By: Governing Body

1. Policy Statement

Rooted in our Christian vision of *Life in All Its Fullness* (John 10:10), we seek to develop digitally responsible citizens who can flourish safely, confidently and respectfully in the online world. We encourage pupils to demonstrate wisdom, integrity, compassion and responsibility in their use of technology and digital communication.

At Bramcote Church of England Primary School, we believe that all children should be able to flourish safely, confidently and responsibly in an increasingly digital world.

Online safety is an integral part of safeguarding and promoting the welfare of children. The school recognises that technology provides significant educational benefits but can also expose children and adults to risks and harm. We therefore adopt a whole-school approach to online safety which is embedded within safeguarding, behaviour, curriculum, leadership and governance.

This policy has been written in accordance with:

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children
- Relationships Education, Relationships and Sex Education (RSE) and Health Education Statutory Guidance
- Teaching Online Safety in Schools
- Education for a Connected World Framework (UKCIS)
- Prevent Duty Guidance
- UK GDPR and Data Protection Act 2018

Online safety concerns will always be treated as safeguarding concerns and responded to through the school's safeguarding procedures.

2. Key Personnel

Role	Name
Headteacher	Sarah Meredith
DSL	Matthew McCallion
Deputy DSLs	Silje Berthelsen
Safeguarding Governor	Vicki Brown
PSHE/RSHE Lead	Abi Bodily
Computing Lead	Silje Berthelsen
IT Support Provider	RMG Systems
Data Protection Officer	PLP Law

3. Aims

This policy aims to:

- safeguard all members of the school community in their use of technology;
- create a culture where online safety is everyone's responsibility;
- educate children to use technology safely, responsibly and confidently;
- minimise risks while maximising learning opportunities;
- ensure robust filtering and monitoring systems are in place;
- provide clear procedures for responding to online safety concerns;
- support parents and carers in keeping children safe online;
- ensure compliance with statutory safeguarding and data protection requirements

4. Scope

This policy applies to:

- pupils;
- staff;
- governors;

- volunteers;
- contractors;
- visitors;
- parents and carers;
- any individual using school systems, devices, networks or digital platforms.

The policy applies both on and off site whenever behaviour has the potential to impact the safety and wellbeing of pupils, staff or the wider school community.

Vulnerable Pupils

The school recognises that some children may be particularly vulnerable to online risks and harm.

Additional consideration may be required for:

- children with SEND;
- looked after and previously looked after children;
- children with social care involvement;
- disadvantaged pupils;
- children experiencing mental health difficulties;
- children who have experienced abuse, neglect or trauma.

Safeguarding responses and educational approaches will be adapted where necessary to ensure all pupils can access support and develop appropriate online safety knowledge and skills.

5. Roles and Responsibilities

Governing Body

The Governing Body will:

- ensure online safety is effectively embedded within safeguarding arrangements;
- ensure effective filtering and monitoring systems are in place;
- receive regular safeguarding reports regarding online safety;
- provide strategic challenge regarding online safety arrangements;
- ensure online safety is adequately resourced;
- monitor compliance with statutory requirements;
- review the effectiveness of this policy annually.

Filtering and Monitoring Oversight

The Governing Body will ensure effective strategic oversight of filtering and monitoring arrangements.

The safeguarding governor will receive regular assurance reports regarding:

- the effectiveness of filtering and monitoring systems;
- safeguarding alerts and actions taken;
- online safety incidents and trends;
- emerging online risks;
- staff training compliance;
- the effectiveness of online safety education.

Governors will provide appropriate challenge and support to ensure online safety arrangements remain effective, proportionate and compliant with statutory safeguarding requirements.

Headteacher

The Headteacher will:

- ensure implementation of this policy;
- promote a safeguarding culture where online safety is prioritised;
- ensure staff receive appropriate training;
- oversee filtering and monitoring arrangements;

- ensure incidents are appropriately managed;
- report significant safeguarding concerns to governors where appropriate.

Safeguarding Lead (DSL)

The DSL has lead responsibility for online safety within safeguarding and will:

- coordinate online safety provision;
- manage online safeguarding concerns;
- liaise with external agencies when required;
- monitor incident trends;
- ensure staff training remains current;
- support pupils and families affected by online harm;
- review filtering and monitoring effectiveness with technical staff;
- ensure safeguarding records are appropriately maintained.

All Staff

All staff will:

Professional Curiosity

Staff will maintain professional curiosity regarding children's online experiences and behaviours.

Staff understand that online activity may provide important indicators of wider safeguarding concerns, including:

- exploitation;
- abuse;
- mental health concerns;
- bullying;
- child-on-child abuse;
- radicalisation;
- neglect.

Where concerns arise, staff will record and report them promptly in accordance with safeguarding procedures.

- understand that online safety is part of safeguarding;
- read and follow this policy;
- report concerns immediately using school safeguarding procedures;
- supervise technology use appropriately;
- model safe and professional online behaviour;
- complete required safeguarding and online safety training;
- maintain professional boundaries online.

Pupils

Pupils are expected to:

- act safely and respectfully online;
- follow school acceptable use expectations;
- report concerns immediately;
- use school technology responsibly;
- respect the privacy and rights of others.

Parents and Carers

Parents and carers are encouraged to:

- support safe technology use at home;
- reinforce school expectations;
- report concerns promptly;
- work in partnership with the school when incidents occur

6. Online Safety Risks

The school recognises that risks continue to evolve rapidly.

Online risks are commonly categorised within the four Cs:

Content

Exposure to harmful, inappropriate, inaccurate or illegal material.

Contact

Harmful interactions with adults or peers.

Conduct

Behaviours that increase risk to self or others.

Commerce

Risks involving money, scams, gambling or exploitation.

Emerging risks may include:

- cyberbullying;
- online abuse;
- online sexual harassment;
- child-on-child abuse;
- radicalisation and extremism;
- grooming;
- exploitation;
- online fraud and scams;
- misinformation and disinformation;
- deepfakes and manipulated images;
- harmful online challenges;
- misogyny and harmful online ideologies;
- livestreaming risks;
- gambling and gaming-related harms;
- sharing of nudes and semi-nudes;
- exposure to violent or hateful content

Online Sexual Extortion (Sextortion)

The school recognises the growing risk of online sexual extortion, commonly known as sextortion.

Sextortion occurs when a child is manipulated, groomed or coerced into sharing sexual images or videos online and is subsequently threatened, blackmailed or pressured.

Any concerns relating to sextortion will be treated as a safeguarding concern and referred immediately to the Designated Safeguarding Lead. The school will work with external agencies, including the Police and Children's Social Care where appropriate, to safeguard affected children.

Pupils will be educated about:

- recognising grooming behaviours;
- safe online relationships;
- reporting concerns early;
- seeking help from trusted adults.

7. Artificial Intelligence (AI)

The school recognises that artificial intelligence (AI) tools are becoming increasingly accessible to pupils, staff and families.

We will:

- promote safe and responsible use of AI;
- teach pupils critical evaluation skills;

- educate pupils about misinformation and AI-generated content;
- ensure staff understand safeguarding risks associated with AI;
- avoid entering confidential or personal information into public AI systems;
- evaluate AI tools before educational use;
- ensure AI use complies with data protection requirements.

Misuse of AI, including bullying, impersonation, creation of harmful content, manipulation of images, academic dishonesty or safeguarding breaches, will be addressed through safeguarding and behaviour procedures.

Generative Artificial Intelligence and Synthetic Media

The school recognises the increasing availability of generative artificial intelligence tools, including chatbots, image generators and synthetic media technologies.

Pupils will be taught to understand that:

- AI-generated content may contain inaccuracies, bias or misinformation;
- not all online content is created by humans;
- images, videos and audio can be manipulated using artificial intelligence;
- deepfakes and synthetic media may be used to deceive, harass or exploit others;
- online information should be critically evaluated before being trusted or shared.

The school will respond appropriately to concerns involving:

- AI-generated bullying or harassment;
- impersonation of pupils or adults;
- the creation or sharing of manipulated images;
- AI-generated indecent imagery;
- misuse of AI to bypass school safeguards;
- academic dishonesty involving AI systems.

8. Online Safety Education

Online safety education is embedded throughout the curriculum.

Children are taught:

- how to stay safe online;
- healthy online relationships;
- privacy and security;
- managing digital footprints;
- recognising scams and manipulation;
- cyberbullying awareness;
- media literacy;
- critical evaluation of content;
- artificial intelligence awareness;
- misinformation and disinformation;
- reporting concerns and seeking help.

The school uses guidance from:

- Education for a Connected World;
- Teaching Online Safety in Schools;
- Relationships Education and Health Education guidance.

Online safety education is delivered through:

- Computing;
- PSHE/RSHE;
- Collective Worship;
- Assemblies;
- Curriculum enrichment;
- Safeguarding events.

9. Filtering and Monitoring

The school recognises filtering and monitoring as a key safeguarding function.

Appropriate filtering and monitoring systems are in place to:

- reduce exposure to harmful content;
- identify safeguarding concerns;
- support safer use of technology;
- protect users from online threats.

Senior leaders, governors, the DSL and technical staff work together to ensure arrangements remain:

- effective;
- proportionate;
- age appropriate;
- regularly reviewed.

The Headteacher, DSL and safeguarding governor understand:

- what is filtered;
- what is monitored;
- what alerts are generated;
- how concerns are escalated;
- how systems contribute to safeguarding.

Filtering and monitoring arrangements are reviewed at least annually and whenever significant changes occur.

The school aims to avoid unnecessary over-blocking that could restrict teaching and learning.

10. Managing Online Safety Concerns

All concerns must be reported immediately to the DSL or Deputy DSL.

Online safety concerns are safeguarding concerns.

Reports may involve:

- cyberbullying;
- harmful content;
- inappropriate contact;
- exploitation;
- grooming;
- self-harm concerns;
- radicalisation;
- online harassment;
- child-on-child abuse;
- sexual violence or harassment.

All incidents will be:

- recorded on CPOMS;
- assessed appropriately;
- investigated proportionately;
- referred to external agencies where necessary.

The school will work with:

- Nottinghamshire Children's Services;
- Police;
- CEOP;
- Prevent teams;
- Local safeguarding partners;
- other relevant agencies.

11. Sharing Nudes and Semi-Nudes

The school follows current UKCIS guidance.

Staff must:

- not view images unnecessarily;
- not share images;
- not delete images;
- immediately inform the DSL.

The DSL will assess risk and determine appropriate action, including referral to external agencies where required.

The welfare of the child will remain central to all decision-making.

12. Child-on-Child Abuse

The school adopts a zero-tolerance approach to child-on-child abuse.

This includes:

- bullying;
- cyberbullying;
- prejudice-based abuse;
- sexual harassment;
- sexual violence;
- image-based abuse;
- online humiliation;
- coercive behaviours.

Children must understand that harmful behaviour online is never acceptable and will be addressed consistently.

13. Social Media

Members of the school community must behave respectfully online.

Staff will:

- maintain professional boundaries;
- avoid online relationships with pupils;
- uphold the reputation of the school;
- follow the Staff Code of Conduct.

Parents are encouraged to raise concerns directly with the school through appropriate channels.

Any social media misuse that impacts safeguarding or school operations may be investigated.

14. Use of Devices

Pupils

A pupil may bring a mobile phone only where agreed by the school. Phones must be handed into the school office on arrival and collected at the end of the day.

Staff

Staff must:

- keep personal devices secure;
- use devices appropriately;
- not access child protection information on personal devices unless specifically authorised;
- follow safeguarding and data protection expectations.

Mobile Phones and Smart Devices

The school recognises that mobile phones, wearable devices, smart watches and other internet-enabled technologies can present both educational opportunities and safeguarding risks.

The use of these devices will be managed in accordance with the school's:

- Mobile Phones and Smart Devices Policy;
- Staff Code of Conduct;
- Child Protection and Safeguarding Policy;
- Acceptable Use Agreements.

Pupils, staff, visitors and volunteers are expected to use personal devices responsibly and in ways which safeguard the welfare, privacy and dignity of all members of the school community.

Visitors and Volunteers

Visitors, volunteers and contractors must not use personal devices in ways that compromise safeguarding arrangements.

15. Digital Images and Media

Photographs and videos will be managed in accordance with:

- safeguarding requirements;
- parental permissions;
- data protection legislation.

Images will be:

- appropriate;
- securely stored;
- used only for authorised purposes.

The school will regularly educate pupils regarding privacy, consent and responsible sharing.

16. Data Protection and Information Security

The school recognises that effective information sharing supports safeguarding.

Staff will:

- follow data protection procedures;
- use approved systems;
- protect sensitive information;
- securely share safeguarding information when necessary.

Concerns regarding data security must be reported immediately.

17. Staff Training

All staff receive:

- safeguarding induction training;
- online safety training;
- filtering and monitoring awareness training;
- regular safeguarding updates;
- updates regarding emerging technologies and online risks.

Governors receive appropriate safeguarding and online safety training to enable effective strategic oversight.

18. Monitoring, Evaluation and Review

The effectiveness of this policy will be monitored through:

- safeguarding audits;
- CPOMS analysis;
- governor monitoring;
- pupil voice;
- staff feedback;
- filtering and monitoring reviews;
- safeguarding reports.

This policy will be reviewed annually or sooner if statutory guidance changes.

Related Policies

- Child Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Mobile Phones and Smart Devices Policy
- Filtering and Monitoring Policy
- Artificial Intelligence Guidance
- Acceptable Use Agreements
- Prevent Duty Policy
- Whistleblowing Policy

Due for Review September 2027