Beckers Green Primary School

Online Safety Policy

Authors: Claire Smyth (Headteacher) & Dan Wright (SAT ICT Hub Manager)
Date: 1st September 2026
Governor Approval Date:
Review Date: September 2027 (Reviewed annually)

1. Statement of Commitment

Beckers Green Primary School is committed to safeguarding and promoting the welfare of all students. Online safety is an essential part of safeguarding and is embedded within the school's culture, curriculum and everyday practice.

The school recognises that digital technologies play an important role in education and communication. While technology provides significant educational opportunities, it can also present risks. The school is committed to ensuring that all members of the school community are protected from potential harm whilst using digital technology.

Online safety forms part of the school's wider safeguarding culture and is considered within safeguarding practice, curriculum planning, staff training and risk assessment activities.

This policy has been developed with reference to Keeping Children Safe in Education 2026, statutory guidance in force from 1 September 2026; Working Together to Safeguard Children; the Prevent duty; the Department for Education's filtering and monitoring standards and guidance on teaching online safety; relevant data protection legislation; and current Department for Education guidance on the safe and effective use of generative artificial intelligence in education.

2. Roles and Responsibilities

Governing Body

The Governing Body is responsible for ensuring that effective online safety arrangements are in place and reviewed regularly.

The school has appointed:

Online Safety Governor: Shane Lake

The Online Safety Governor will receive regular updates regarding:

- Online safety incidents and trends.
- Filtering and monitoring arrangements.
- Safeguarding concerns linked to online activity.
- Staff training and awareness.
- Outcomes of annual online safety reviews.
- Ensuring that all staff, including those who do not work directly with children, read and understand Part One of KCSIE 2026 and any further sections relevant to their role.

Headteacher

The Headteacher has overall responsibility for online safety and will ensure that:

- Appropriate online safety arrangements are implemented and monitored.
- Concerns are acted upon appropriately and without delay.
- Staff receive suitable training.
- All staff understand their safeguarding responsibilities under KCSIE 2026, including what to do if they have concerns about a child, another adult, or safeguarding practice within the school.

- Online safety is embedded throughout the curriculum.
- Filtering and monitoring arrangements remain effective.

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Managing online safeguarding concerns.
- Assessing risk and determining appropriate action.
- Maintaining safeguarding records.
- Liaising with external agencies where required.
- Supporting staff to recognise online indicators of abuse, neglect and exploitation, including child-on-child abuse, harmful sexual behaviour, grooming, exploitation, radicalisation, cybercrime and serious violence.

SAT Central ICT Team

ICT services are provided and maintained by the **SAT Central ICT Team**.

The SAT Central ICT Team supports the school through:

- Secure ICT infrastructure management.
- Cyber security controls.
- Device management and security.
- Filtering and monitoring solutions.
- Technical support and incident response.
- Guidance on compliance and emerging risks.

Dan Wright, SAT ICT Hub Manager, and/or a nominated SAT Central ICT Team representative will support the school's online safety arrangements and contribute to termly reviews.

Online Safety Group

The school operates an Online Safety Group which meets at least termly.

Membership may include:

- Headteacher
- DSL
- Online Safety Governor
- Dan Wright, SAT ICT Hub Manager, and/or nominated SAT Central ICT Team representative
- Other relevant staff as appropriate

The group will review:

- Online safety incidents and trends.
- Filtering and monitoring effectiveness.
- Staff awareness and training.
- Emerging online safety risks.
- Progress against identified actions.

3. Education and Awareness

Online safety education is planned and delivered throughout the curriculum and wider school life.

The school recognises that children with Special Educational Needs and Disabilities (SEND) may be particularly vulnerable to online risks due to factors such as communication difficulties, social vulnerabilities, or differing levels of understanding. The school is committed to providing appropriate support, education, and safeguarding measures to ensure that all students, including those with SEND, can access online technologies safely and responsibly.

Online safety education addresses risks associated with **content, contact, conduct and commerce**, ensuring students develop the knowledge and skills required to navigate online environments safely and responsibly.

Students are taught age-appropriate knowledge and skills including:

- Safe and responsible use of technology.
- Online relationships.
- Respectful online behaviour.
- Cyberbullying and how to report concerns.
- Privacy and personal information.
- Digital footprints and online reputation.
- Misinformation, disinformation and fake content.
- Online scams and manipulation.
- Healthy and balanced use of technology.
- How and where to seek help.
- Age-appropriate understanding of emerging technologies, including artificial intelligence.
- Understanding the benefits and risks of generative artificial intelligence, including accuracy, bias, privacy, age-appropriateness, harmful content and responsible use.

Online safety education is delivered through Computing, PSHE, Project Evolve and other curriculum opportunities.

The school will also seek opportunities to support parents and carers in promoting safe and responsible technology use.

Further information and practical guidance for parents and carers on supporting children to use the internet and connected technology safely and responsibly is available in the Online Safety section of the school website.

Parents and carers are asked through Arbor to confirm that they have read and understood this Online Safety Policy, acknowledge the school's expectations for their child's safe and responsible use of the internet and digital technology, and agree to support these expectations at home and elsewhere.

4. Filtering and Monitoring

The school maintains appropriate filtering and monitoring arrangements in line with current Department for Education requirements.

The school uses:

- **Smoothwall** filtering and monitoring solutions.
- **Impero Education Pro** classroom management and safeguarding monitoring software.

The Governing Body has strategic responsibility for ensuring that appropriate filtering and monitoring systems and processes are in place. The Headteacher, the DSL and the SAT Central ICT Team have clearly assigned operational and technical responsibilities for overseeing these arrangements, reviewing safeguarding alerts and ensuring that systems remain effective in protecting students from harm.

These systems help support safeguarding by identifying potentially harmful, inappropriate or unsafe online activity.

Monitoring arrangements may assist in identifying indicators associated with:

- Bullying and cyberbullying.
- Self-harm concerns.
- Mental health and wellbeing concerns.
- Child-on-child abuse.
- Extremism and radicalisation.
- Sexual harassment.
- Safeguarding concerns requiring further review.

Impero may generate alerts based on online activity and safeguarding-related keywords. Alerts are reviewed by appropriate staff and referred to the DSL where necessary.

Filtering and monitoring systems support safeguarding but do not replace professional curiosity, professional judgement or staff vigilance.

Filtering and monitoring arrangements will be reviewed regularly to ensure they remain effective, proportionate and appropriate to the school's safeguarding needs.

Filtering and monitoring provision will be reviewed at least annually and whenever there is a significant safeguarding, technical or contextual change. The review will be documented and reported to the Governing Body. It will consider whether responsibilities are clear; whether illegal, inappropriate and potentially harmful content, including AI-generated content, is restricted without unreasonably affecting teaching and learning; whether monitoring is effective; whether staff understand the systems in place; and whether alerts, decisions and actions are recorded and followed up.

For security reasons, detailed technical configurations and cyber security measures are not included within this policy.

5. Staff Training and Cyber Security

All staff and governors receive regular online safety and cyber security awareness training.

The school uses **usecure** to provide:

- Cyber security awareness training.
- Phishing simulation exercises.
- Password security awareness.
- Data protection awareness.
- Guidance on emerging cyber risks and threats.

Staff and governors are expected to apply this learning in practice and contribute to maintaining a secure and safe digital environment for students and colleagues.

6. Use of Technology

This policy applies to students, staff, governors, volunteers, visitors and contractors when accessing school systems or working within the school environment. All users are expected to use technology safely, responsibly and appropriately.

Users must:

- Protect login credentials and keep passwords confidential.
- Use authorised systems and services.
- Respect the privacy and safety of others.
- Report concerns promptly.
- Use technology in a manner consistent with safeguarding principles.

The school may monitor the use of school systems where lawful and appropriate for safeguarding, security, operational or investigative purposes.

The school will maintain appropriate information security and access management arrangements, including proportionate controls for user accounts, passwords, multi-factor authentication where appropriate, device security, system access, data protection and the prompt removal or adjustment of access when roles change.

Any generative AI product or service proposed for use in school must be assessed and approved before use, taking account of its intended purpose, age suitability, accessibility and SEND needs, safeguarding features, privacy and data protection, security, intellectual property, accuracy and bias, and the Department for Education's generative AI product safety standards. Personal, special category, safeguarding or confidential information must not be entered into an unapproved AI service. Staff remain professionally responsible for checking AI-generated outputs and must not rely on them to make safeguarding decisions.

7. Mobile Devices, Photography and Personal Information

The use of mobile phones and similar devices is governed by the Beckers Green Primary School Mobile Phone Policy. This section should be read alongside that policy, which sets out the detailed requirements for students, staff, parents/carers, visitors and volunteers.

Students must not use mobile phones or smartwatches during the school day. A student may bring a mobile phone onto the school site only with the Headteacher's permission, including where agreed for safety or other exceptional circumstances. Any permitted phone must be handed to the school office on arrival and collected at the end of the school day, in accordance with the Mobile Phone Policy.

Staff must follow the Mobile Phone Policy when using personal or school-provided mobile devices. Personal mobile phones must not be used while students are present, except where the Headteacher has approved special arrangements or where limited professional use is permitted by that policy, such as multi-factor authentication, emergency evacuation or supervision of off-site or residential visits. Staff must not use personal mobile phones to process personal or confidential school information, contact students or parents/carers, or take photographs or recordings of students, their work or anything else that could identify a student.

Where photographs or recordings are required for an authorised lesson, school trip or activity, school equipment must be used. Photographs, videos and personal information must be collected, stored, used and shared responsibly and in accordance with legal requirements, consent arrangements and the school's relevant policies.

The school will take reasonable steps to ensure that personal information is protected and that images of students are used appropriately.

8. Reporting Concerns

All online safety concerns must be reported without delay.

Concerns may include:

- Access to inappropriate content.
- Cyberbullying.
- Online abuse or exploitation.
- Harmful or concerning communications.
- Safeguarding concerns identified through monitoring systems.
- Online grooming concerns.
- Extremist content.
- Suspected criminal activity.
- Data protection incidents.

Safeguarding concerns must be referred immediately to the DSL or a deputy DSL. If a child is in immediate danger or at risk of immediate harm, staff must follow the school's child protection procedures and contact the emergency services without delay where required.

All online safety incidents and concerns will be recorded using the school's safeguarding recording system and managed in accordance with safeguarding procedures.

Records of online safety concerns are reviewed periodically to identify trends, emerging risks and opportunities for preventative education and safeguarding intervention.

Where necessary, concerns may be referred to appropriate external agencies.

Where a concern or allegation involves a member of staff, supply staff, volunteer, governor, contractor or another adult working with or around children, staff must follow the school's child protection procedures without delay. Concerns about an adult should be reported to the Headteacher; concerns about the Headteacher should be reported to the Chair of Governors. Low-level concerns must be reported through the route set out in those procedures.

9. Monitoring, Review and Audit

The effectiveness of the school's online safety arrangements will be reviewed regularly.

An annual Online Safety Audit will be completed, considering:

- Online safety education.
- Staff awareness and training.
- Filtering arrangements.
- Monitoring arrangements.
- Cyber security awareness.
- Safeguarding incidents and trends.
- Emerging risks and recommended actions.

Findings and actions will be reported to senior leaders and governors and reviewed through the Online Safety Group.

The school will retain evidence of policy review, staff training, governor oversight, filtering and monitoring checks, incident trends, actions taken and communication with students, parents and carers to demonstrate that the policy is implemented in practice.

Commitment

Beckers Green Primary School is committed to ensuring that technology is used safely, responsibly and effectively to support learning, wellbeing and safeguarding for all members of the school community.