

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 pupils. 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, which comes into force on 1 September 2026, Department for Education filtering and monitoring standards, Working Together to Safeguard Children, the Prevent Duty, relevant data protection legislation and current Department for Education guidance on the safe and effective use of 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 the relevant safeguarding information in Part One of KCSIE 2026.

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.

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

Pupils 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 (Jigsaw scheme), Project Evolve and other curriculum opportunities.

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

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.

Senior leaders, the DSL and the SAT Central ICT Team work together to oversee filtering and monitoring arrangements, review safeguarding alerts and ensure that systems remain effective in protecting pupils 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 following any significant safeguarding, technical or contextual change. Reviews will consider whether responsibilities are clear, whether harmful and inappropriate content is being blocked without unreasonably restricting teaching and learning, whether monitoring is effective, and whether 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 pupils and colleagues.

6. Use of Technology

This policy applies to pupils, 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.

7. Mobile Devices, Photography and Personal Information

The use of mobile devices must support safeguarding and professional standards.

Pupils who are permitted to bring mobile phones to school must hand them to the school office at the beginning of the school day and collect them at the end of the school day in line with Mobile Phone Policy and written agreement from parents.

Staff should use school-approved systems and devices for professional activities wherever possible.

Photographs, videos and personal information will be collected, stored, used and shared responsibly and in accordance with legal requirements.

The school will take reasonable steps to ensure that personal information is protected and that images of pupils 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.

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 involves a member of staff, supply staff, volunteer, governor, contractor or another adult working with or around children, staff must follow the school's safeguarding

procedures for concerns or allegations about adults, including low-level concerns, and report without delay to the appropriate senior leader or designated route.

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 pupils, 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.

Appendix A

Pupil Acceptable Use Agreement

Beckers Green Primary School

Pupil Acceptable Use Agreement

At Beckers Green Primary School, we use technology to help us learn, create and communicate safely.

When using school technology, I agree to:

- Be kind, respectful and responsible online.
- Use technology only for learning and approved school activities.
- Keep my passwords private and not share them with anyone.
- Tell a trusted adult if I see or hear something online that worries me, upsets me or feels unsafe.
- Respect other people's work, privacy and feelings.
- Look after school equipment and use it carefully.
- Never try to access websites, apps or content that I know are not suitable for children.
- Never use technology to hurt, upset, bully or exclude others.
- Never share personal information about myself or other people without permission.
- Follow instructions given by school staff when using technology.

I understand that school devices and systems may be monitored to help keep everyone safe.

I understand that if I do not follow these rules, my use of technology may be restricted and further action may be taken by the school.

Pupil Declaration

I have read, discussed and understood these expectations.

Pupil Name: _____

Class: _____

Pupil Signature: _____

Date: _____

Appendix B

Parent / Carer Online Safety Acknowledgement

Beckers Green Primary School

Parent / Carer Online Safety Acknowledgement

Beckers Green Primary School uses digital technology to support teaching, learning, communication and safeguarding.

The school is committed to helping pupils use technology safely and responsibly through education, appropriate filtering and monitoring arrangements, staff training and safeguarding procedures.

Parents and carers play an important role in supporting children to stay safe online and are encouraged to:

- Talk regularly with their child about online safety.
- Promote positive and responsible use of technology at home.
- Support the school's expectations for safe online behaviour.
- Encourage their child to report any online concerns to a trusted adult.
- Contact the school if they have concerns about their child's online safety or wellbeing.

By signing below, I confirm that:

- I have read the school's Online Safety Policy.
- I understand the school's approach to online safety.
- I will support my child in using technology safely and responsibly.
- I understand that the school uses appropriate filtering and monitoring systems to help safeguard pupils.
- I will inform the school of any significant online safety concerns affecting my child.

Parent / Carer Declaration

Parent / Carer Name: _____

Name of Child: _____

Signature: _____

Date: _____