EAVES PRIMARY SCHOOL

Online Safety Policy

Policy owner: Headteacher and Designated Safeguarding Lead

Prepared: November 2026

Approval: Governing Body – Approved 24.11.2026

Next review: November 2027, or earlier following changes to guidance or school systems

1. Statement of intent

At Eaves Primary School, we want children to benefit from technology while learning how to use it safely, responsibly and confidently. Online safety is part of our safeguarding culture, curriculum and everyday expectations: Ready, Responsible, Resilient and Respectful. We recognise that online and offline risks often overlap, and that no filtering system replaces effective adult supervision, education and prompt safeguarding action.

2. Legal and guidance framework

This policy reflects Keeping Children Safe in Education (KCSIE) 2026, Working Together to Safeguard Children, the Prevent duty, the Education Act 2002, the Data Protection Act 2018 and UK GDPR, relevant DfE guidance on teaching online safety and generative AI, and the DfE filtering and monitoring standards updated in September 2026. It is reviewed alongside the school's safeguarding policy. Where legislation or statutory guidance changes, current requirements take precedence.

3. The four areas of online risk

Content: harmful, illegal, misleading or age-inappropriate material, including extremist content and AI-generated imagery.

Contact: harmful interaction, grooming, exploitation, coercion and unwanted contact.

Conduct: bullying, harassment, unsafe sharing, image-based abuse and behaviour that harms others.

Commerce: scams, phishing, gambling-like features, harmful advertising and financial exploitation.

Staff also consider risks arising from social media, gaming, messaging, live streaming, smart devices and emerging technology.

4. Roles and responsibilities

The governing body ensures online safety is reflected in safeguarding arrangements, scrutinises filtering and monitoring assurance, and receives appropriate reports. The safeguarding governor is Mike Williams.

The Headteacher, Mrs Lawrenson, ensures clear procedures, staff training, resources and oversight.

The Designated Safeguarding Lead (DSL), Mrs Lloyd, takes lead responsibility for online safety and responding to online safeguarding concerns. Deputy DSLs are Mrs Lawrenson, Mrs Leavesley and Mrs Bowles. The DSL works with the SENDCo and technical support where risks require additional action.

The school's IT support/provider implements and maintains technical controls, communicates failures and limitations, and provides evidence for review. Technical support does not replace the DSL's safeguarding decision-making.

All staff supervise technology use, follow acceptable-use rules, challenge unsafe behaviour and report concerns immediately. Pupils are taught to seek help and to use technology respectfully. Parents and carers are encouraged to work with the school.

5. Filtering and monitoring

Eaves maintains appropriate filtering and monitoring arrangements on school networks and school-managed devices, supported by external assurance. The Headteacher, DSL and technical provider will establish and document who manages filtering, who receives and reviews monitoring alerts, escalation routes and cover arrangements. The DSL leads on safeguarding responses to alerts.

Filtering should restrict access to illegal and harmful material without unnecessarily blocking learning. Monitoring should identify concerning activity in a timely way. Staff must continue active, in-person supervision of devices and report anything concerning even where no alert is generated.

The school will carry out and record at least an annual review of filtering and monitoring effectiveness, with further reviews following significant changes or incidents. The review considers pupil age and needs, SEND, devices used off site, guest access, AI-enabled services, technical limitations, incident patterns and staff feedback. Checks and remedial actions are recorded, assigned and followed up. The school will confirm that monitoring arrangements are explained in relevant privacy notices and that any required data protection impact assessment is completed.

6. Reporting and responding to concerns

Any pupil disclosure or online safety concern must be passed to the DSL without delay and recorded factually on CPOMS, in line with safeguarding procedures. If there is immediate danger, staff take urgent protective action and contact emergency services as necessary. Staff should not promise secrecy, investigate independently, forward harmful imagery or ask children to repeat distressing accounts unnecessarily.

The DSL assesses the risk, supports the child, preserves relevant evidence lawfully, considers parents/carers and decides whether children's social care, police, Prevent or specialist services need to be involved. Staff must not view, copy or share nude or semi-nude images of children unless specifically authorised by relevant safeguarding guidance and advice; the DSL follows the appropriate UKCIS procedures.

Online bullying, harassment and harmful sexual behaviour are addressed through safeguarding, child-on-child abuse and behaviour procedures. Concerns about staff online conduct are reported to the Headteacher, or to the Chair of Governors where the concern is about the Headteacher, under the allegations and low-level concerns procedures. Incidents are reviewed for patterns and lessons learned.

7. Teaching online safety

Online safety is taught progressively through computing, Jigsaw PSHE, relationships and health education, assemblies, Picture News and safeguarding discussions. Teaching includes trusted adults, privacy, passwords, respectful communication, cyberbullying, reliable information, misinformation, scams, consent, image sharing, age limits, online pressure and how to report concerns.

EYFS and younger pupils learn simple routines such as asking an adult before using a link, keeping personal details private and telling a trusted adult when something worries them. Older pupils build understanding of digital footprints, manipulation, online relationships, exploitation and safe decision-making. Staff adapt teaching and support for children with SEND, communication needs or additional vulnerability. Pupils are not exposed to harmful material simply to demonstrate a risk.

8. Acceptable use and classroom technology

School devices, accounts, apps and online services are used for authorised educational purposes. Staff select age-appropriate resources, check privacy and safeguarding risks before use, and ensure pupils are supervised. Pupils must not share passwords, bypass controls, access others' accounts, contact strangers or post images without permission. Breaches are handled proportionately with safeguarding needs considered first.

Personal mobile devices, smart watches, cameras and removable media are subject to school rules and staff professional boundaries. Staff must not use personal accounts to communicate privately with pupils. Images of children are captured, stored and published only through approved arrangements and permissions. Remote or home learning using school-managed technology follows the same safeguarding expectations.

9. Artificial intelligence and emerging risks

The school assesses educational and safeguarding risks before adopting AI-enabled tools. Staff must not enter identifiable or sensitive pupil information into unapproved systems, and must check the accuracy, suitability and age appropriateness of generated content. Pupils use AI tools only where specifically authorised and supervised. The school recognises risks from deepfakes, impersonation, synthetic sexual imagery, persuasive chatbots, misinformation and data collection; concerns are reported through safeguarding procedures. Filtering and monitoring reviews consider AI content and platforms.

10. Cyberbullying, exploitation and harmful content

The school responds to online incidents even when they happen away from school if they affect pupil welfare or school life. This includes bullying through messaging and gaming, coercion, grooming, radicalisation, harmful challenges, fraud and exposure to violent or sexual content. Responses prioritise the child's safety, appropriate support, evidence preservation and proportionate action. Staff do not amplify hoaxes or harmful challenges unnecessarily. Where cybercrime concerns arise, the DSL considers appropriate specialist advice and referral.

11. Families and the wider community

Eaves shares age-appropriate guidance with families about parental controls, gaming, social media age restrictions, online friendships, reporting concerns and balancing screen use. Parents are encouraged to speak with the class teacher or DSL about worries. Visitors and external providers

using technology with pupils must follow school safeguarding and acceptable-use expectations. School communications and social media must protect pupils' privacy and dignity.

12. Staff training and assurance

All staff read KCSIE 2026 Part One and receive safeguarding training that includes online safety and filtering and monitoring responsibilities. New staff and volunteers receive relevant induction. The DSL and school leaders maintain suitable knowledge of emerging risks; staff receive updates as needed. The governing body reviews the policy annually and receives assurance on safeguarding incidents, curriculum provision, staff training and technical controls, without unnecessary disclosure of personal data.

13. Monitoring and review

The Headteacher and DSL review implementation through safeguarding records, pupil voice, curriculum monitoring, technical assurance, training and feedback from families. This policy will be reviewed by November 2027 or sooner following significant incidents, changes in technology, school practice or statutory guidance.

Appendix A: Immediate response for staff

- Listen calmly and reassure the child; do not promise confidentiality.
- If there is immediate danger, act at once and seek emergency help.
- Report the concern to Mrs Lloyd (DSL) or a deputy DSL without delay.
- Record factual details on CPOMS; do not independently investigate or circulate harmful images.
- Follow DSL advice on safeguarding action, parents, referrals and evidence.

Appendix B: Pupil acceptable-use expectations

- I use school technology when an adult says it is appropriate.
- I keep my personal information and passwords private.
- I am kind and respectful when I communicate online.
- I do not open, share or send anything that could hurt or upset someone.
- If something worries me, I stop and tell a trusted adult.