

Abingdon Primary School



Digital Resilience Policy



Status and Review	Term	Year
Last Review date	Autumn	2026
Next Review	Autumn	2027
Lead	Adam Cooper (Headteacher)	Raj Kaur (Digital safeguarding lead)

1. Purpose and principles

This policy applies to pupils, employees, governors, volunteers, contractors, parents/carers and community users accessing school technology or representing the school online. Digital resilience means the knowledge, skills and confidence to recognise and manage online risks, seek help, recover from setbacks and participate positively and safely in digital life.

Safeguarding is everyone's responsibility, including where harm originates outside school.

The policy operates alongside the Trust child protection and safeguarding policy, behaviour and anti-bullying policies, staff code of conduct, acceptable use agreements (AUPs), data protection and retention policies, information security, SEND, RSHE and complaints procedures. If any provision conflicts with current statutory guidance, safeguarding and statutory requirements take precedence.

2. Legal and guidance framework (England)

- Keeping Children Safe in Education (KCSIE) 2026 (statutory; effective September 2026): safeguarding, online risks, child-on-child abuse, reporting and oversight. All staff must read Part One in full.
- Education Act 2002 safeguarding duties; Children Act 1989 and 2004; Working Together to Safeguard Children (current version).
- Online Safety Act 2023: statutory duties principally imposed on regulated online services; not a substitute for school safeguarding, filtering or curriculum obligations.
- UK GDPR and Data Protection Act 2018 as amended, including relevant changes introduced by the Data (Use and Access) Act 2025; DfE data protection in schools guidance updated October 2026.
- DfE digital and technology standards (updated September 2026), including filtering and monitoring and cyber security core standards.
- DfE statutory Mobile phones in schools guidance, issued June 2026 and applicable from September 2026.
- DfE generative AI in education guidance, AI product safety standards (January 2026), and AI/data protection guidance; UKCIS sharing nudes and semi-nudes advice (March 2024).



3. Governance, accountability and assurance

3.1 Governors and Trust

- Approve and review this policy; ensure sufficient resources, training, effective safeguarding arrangements and appropriate filtering and monitoring.
- Receive at least annual assurance on online safeguarding, AI adoption, incidents, cyber risks, filtering/monitoring reviews and progress towards DfE standards.
- Ensure clear accountability between school leadership, Trust IT, technical suppliers and the Data Protection Officer (DPO).

3.2 Headteacher, DSL and Computing Lead

- The Headteacher is accountable for implementation, staff conduct, incident escalation and appropriate oversight.
- The DSL leads safeguarding responses, records and referrals; considers the four online risk categories: content, contact, conduct and commerce.
- The Computing Lead plans progressive digital resilience teaching and coordinates with the DSL on emerging risks, AI literacy and parental information.
- The designated senior digital lead and IT provider maintain risk registers, security controls, service inventories, monitoring arrangements and tested recovery plans.

3.3 Staff, pupils and parents

All staff follow AUPs, supervise digital activity, report concerns immediately, keep credentials secure, check information before sharing and use only approved services. Pupils follow age-appropriate agreements and know how to report concerns without fear of blame. Parents and carers are supported with practical online safety advice and know the school's reporting routes.

4. Safeguarding online and responding to concerns

All online concerns, including those occurring at home but affecting a pupil, are reported promptly to the DSL using the school's approved safeguarding recording system. Staff must not investigate independently, promise secrecy, or circulate harmful content. The DSL assesses immediate safety, records decisions and contacts children's social care, police or other agencies as required. In an emergency call 999; otherwise follow locally agreed referral routes and the safeguarding policy.

Online risks include grooming, coercion, exploitation, harmful sexual behaviour, cyberbullying, scams, harmful or extremist content, online hate, self-harm content, impersonation, location sharing, live streaming and AI-generated manipulation. Children with SEND or additional vulnerabilities may require adapted support and teaching.



4.1 Sexual images, AI deepfakes and harmful imagery

Any incident involving nude or semi-nude images of children, including digitally manipulated or AI-generated images, is an immediate safeguarding matter. Staff must NOT view, copy, download, print, forward, save or delete images, nor ask children to send or delete them. Refer to the DSL immediately; only the DSL may determine any exceptional viewing under UKCIS guidance. Preserve information without handling imagery, support the child, assess coercion and exploitation, and involve parents unless this increases risk. The DSL determines police/social care referrals and appropriate takedown support.

5. Filtering, monitoring and internet access

The Trust and school will maintain age-appropriate filtering and effective monitoring across school-managed systems, including cloud services, devices and approved AI products. Systems must block harmful material without unreasonably restricting educational content. The DSL, IT lead and governor/trust representatives will review effectiveness at least annually and following significant changes or incidents, document findings and actions, and ensure monitoring alerts have named responders and cover arrangements.

- Keep an inventory of filtering and monitoring providers, coverage, exclusions, alerts, escalation routes and known limitations, including off-site use.
- Risk assess generative AI tools, including prompts, outputs, conversational interactions, image generation, age suitability and whether filtering and monitoring apply.
- Staff must not bypass controls; requests for educational exceptions require documented authorisation and review.
- Explain proportionate monitoring to users through privacy notices and AUPs; protect sensitive monitoring logs with role-based access.



6. Cyber security, continuity and data protection

The school will work towards DfE core digital and technology standards by 2030, while meeting current statutory safeguarding obligations now. The IT provider and leadership will conduct a cyber risk assessment annually, review it each term, maintain a cyber awareness plan, secure accounts with appropriate multi-factor authentication, apply least-privilege access, maintain supported software, backups and recovery testing, and document incident response.

High-risk or critical vulnerabilities and unrated vendor fixes will be addressed in line with the DfE cyber security standard, normally within 14 days of release. Staff report phishing, suspected compromise, lost devices and data breaches immediately. The DPO assesses personal data incidents and any ICO notification requirement and deadlines. No member of staff may independently disclose pupil or staff personal information through unapproved apps or AI tools.

Personal data is collected and used only with a lawful basis, transparency, minimisation, retention and security controls. School images, video, voice recordings and biometric or special-category data require specific assessment and applicable permissions/lawful bases. Publication permissions are distinct from data protection lawful bases. The Trust DPO will review relevant 2026 Data (Use and Access) Act changes and update notices, requests and procedures as necessary.

7. Artificial intelligence (AI): safe and responsible use

7.1 Approval and procurement

No AI product or feature may be used with pupils or school data until approved through the Trust/school procurement and risk assessment process, with input from the DSL, DPO, IT lead and curriculum lead. The assessment considers educational purpose, minimum age and terms, data processing and international transfers, retention, model training, accessibility, bias, accuracy, copyright, content moderation, child safety and filtering/monitoring. Consider a data protection impact assessment (DPIA) where processing is likely high risk. Maintain an approved AI tools register and review it regularly.



7.2 Staff use

- Use AI to assist planning, resource adaptation, accessibility or administrative drafting only when approved and with professional oversight. Staff remain accountable for all outputs and decisions.
- Do not enter identifiable pupil, parent, staff, safeguarding, medical, SEND, assessment or confidential Trust information into public or unapproved AI systems. Use anonymised or synthetic examples where appropriate; even approved processing requires a lawful basis and data minimisation.
- Check AI-generated information for factual errors, bias, discriminatory language, copyright/licensing concerns and suitability for pupils before use.
- Do not use AI alone to make safeguarding, disciplinary, SEND, admissions, assessment or other consequential decisions about children. Human review is mandatory.
- Do not create realistic synthetic images, voice clones or impersonations of identifiable pupils or staff without a specific approved lawful purpose and risk assessment.

7.3 Pupil use

Primary pupils must not independently access open-ended consumer generative AI chatbots or image generators through school systems. Any pupil-facing AI activity requires an approved, age-appropriate tool, a clear educational purpose, direct adult supervision and safeguarding controls. Account creation must comply with service age limits and school authorisation. Staff must offer an alternative where appropriate.

7.4 AI literacy and academic integrity

Pupils will learn, in developmentally appropriate ways, that AI can generate plausible but false information, fabricated pictures, misleading voices and biased responses; that real people can be harmed by impersonation; and that private information should not be entered into online tools. Teachers will model checking claims against trusted sources and recognising when work is AI-assisted. Staff will explain acceptable assistance for tasks and ensure learning and assessment remain authentically the pupil's.

7.5 AI incidents

Suspected AI-generated sexual imagery, impersonation, bullying, unsafe chatbot advice, personal data disclosure or other harm must be reported promptly to the DSL; technical/data concerns also go to IT and the DPO. Suspend access when necessary, record the service and relevant circumstances without reproducing illegal images, preserve appropriate system logs and follow safeguarding, breach and takedown procedures.



8. Mobile phones, cameras, social media and communication

In line with statutory guidance effective September 2026, pupils must not use mobile phones during the school day, including lessons, breaks and lunchtime, subject to documented exceptions for medical, disability or other justified individual needs. School arrangements for devices brought onto site, storage, collection and sanctions must be communicated to families and reflected in the behaviour policy. Staff device use and photographs are governed by the staff code of conduct and school-approved systems. Staff use only authorised school accounts and communication platforms for contact with pupils and families; personal messaging and private social media contact are prohibited except where a formally approved safeguarding or operational arrangement permits. Pupil photographs, recordings and names are published only under school/Trust procedures. Avoid identifiable metadata, locations and unnecessary sharing. Cyberbullying and online allegations are managed under safeguarding, anti-bullying and staff-allegations procedures.

9. Teaching digital resilience across the primary curriculum

Digital resilience is taught through Computing, relationships/health education, PSHE, assemblies and relevant subjects, revisited progressively and adapted for pupils with SEND. Teaching is calm, practical, inclusive and avoids graphic or fear-based examples.

EYFS / Key Stage 1

- Trusted adults, asking permission, kindness online and recognising when something feels wrong.
- Keeping names, photos, passwords and personal details private; stopping and telling an adult.
- Understanding that pictures and stories online may be changed or made up.

Key Stage 2

- Privacy settings, strong passwords, scams, phishing, advertising, in-app purchases and reporting/blocking.
- Cyberbullying, respectful communication, consent before sharing images, grooming warning signs and online influence.
- Evaluating sources, misinformation, AI-generated text/images/audio, bias, deepfakes and responsible research.



12. Official sources and reference links

KCSIE 2026 — <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

DfE digital and technology standards — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>

Filtering and monitoring core standard — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

Cyber security core standard — <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard>

Mobile phones in schools statutory guidance —

<https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools>

Generative AI in education — <https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>

AI product safety standards — <https://www.gov.uk/government/publications/generative-ai-product-safety-standards/generative-ai-product-safety-standards>

AI and data protection in schools — <https://www.gov.uk/guidance/data-protection-in-schools/generative-artificial-intelligence-ai-and-data-protection-in-schools>

Data protection in schools updates — <https://www.gov.uk/guidance/data-protection-in-schools/updates>

UKCIS sharing nudes and semi-nudes guidance —

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

AI support materials for schools — <https://www.gov.uk/government/collections/using-ai-in-education-settings-support-materials>

Appendix A. Summary of significant changes from Summer 2025 policy

- Retained the original policy's emphasis on resilience, responsibility, curriculum, internet controls, cyberbullying, radicalisation, gaming, safeguarding and reporting.
- Updated the statutory baseline from the 2025 review to KCSIE 2026 and September 2026 filtering/cyber standards.
- Added full AI governance, procurement, pupil access, staff practice, AI literacy, deepfake harms and AI incident response.
- Updated phone rules to reflect statutory mobile phone guidance from September 2026.
- Replaced the original detailed staff device-search instructions with a referral-first approach consistent with UKCIS imagery guidance; DSLs should consult current search powers separately.
- Added 2026 data protection change review, clearer governor assurance and operational implementation checklist.



