



“Enabling life in all its fullness”

“I came that you may have life, life in all its fullness” (John10:10)

Our **Core Christian values** for our school are: *Perseverance, Creativity, Trust and Friendship.*

E-SAFETY / ONLINE SAFETY POLICY

2026–2027

Approved by Governors: September 2026

Review Date: September 2027 or sooner following significant guidance, technology or safeguarding change

Related policies Safeguarding and Child Protection; Behaviour; Anti-Bullying; Acceptable Use; Data Protection/Privacy; RSE/RSHE; Staff Code of Conduct; Mobile Phone; Complaints; SEND; Remote Learning

Policy statement

Ashton Keynes CE Primary School recognises that technology is an essential part of pupils’ learning, communication and everyday lives.

Our Christian vision, “Life in all its fullness” (John 10:10), commits us to helping every child flourish safely, confidently and responsibly.

This policy sets out how the school promotes online safety, prevents and responds to online harm, and uses filtering, monitoring, education, safeguarding and appropriate technical controls to protect pupils and staff.

Online safety is a whole-school safeguarding responsibility. It applies to all pupils, staff, governors, volunteers, visitors, contractors and anyone using school systems, devices or networks, whether on or off the school premises.

Statutory and regulatory framework

This policy should be read alongside the current versions of:

- Keeping Children Safe in Education (KCSIE) 2026, including the online safety and filtering and monitoring requirements.
- Education Act 1996 and related safeguarding duties.
- Children Act 1989 and 2004.
- Equality Act 2010 and Public Sector Equality Duty.
- Data Protection Act 2018 and UK GDPR.
- Computer Misuse Act 1990.
- Prevent duty guidance and the school's safeguarding procedures.
- Department for Education Meeting digital and technology standards in schools and colleges: Filtering and monitoring – core standard, current 2026 version.
- Department for Education guidance on generative AI and product safety where AI tools are used.
- Ofsted state-funded school inspection toolkit applicable from September 2026.

Scope

This policy covers internet use, school-managed devices, tablets, laptops, interactive displays, email, messaging, cloud platforms, learning platforms, social media, gaming, apps, video-sharing services, artificial intelligence and generative AI, digital photography/video, online communication, remote learning and personal devices when they affect school life or safeguarding.

Roles and responsibilities

Governing Body: Provides strategic oversight; ensures online safety is embedded in safeguarding; receives assurance about filtering and monitoring; ensures appropriate resources, training and review; challenges leaders where necessary.

Headteacher / SLT: Has overall operational responsibility; ensures policy implementation, staff training, risk assessment, incident response and annual review; ensures online safety is considered in procurement and introduction of new technology.

Designated Safeguarding Lead (DSL): Leads safeguarding responses to online concerns; reviews relevant filtering/monitoring alerts and reports; ensures concerns are recorded and referred in line with safeguarding procedures; provides governor assurance.

Filtering/Monitoring lead and IT provider: Maintain appropriate filtering and monitoring, provide reports, investigate technical concerns, ensure systems work on managed devices and support incident response. Responsibilities must be documented even where IT is outsourced. This Mr. Dan Hockaday working with Oakford Technologies our IT Provider.

All staff: Supervise pupils; model safe digital behaviour; complete required training; report concerns immediately; follow acceptable-use, safeguarding and data-protection requirements. Computing and Technology Lead is: Miss Josie Chomicz. She has a team of digital pupil leaders.

Pupils: Use technology responsibly; follow school rules; report anything worrying, harmful or inappropriate; respect privacy, consent and others' dignity.

Parents/carers: Support safe technology use at home, supervise age-appropriate use, understand school expectations and report significant online safeguarding concerns.

Governors, volunteers and visitors: Follow the school's acceptable-use requirements and report concerns through the school's safeguarding arrangements.

Online safety education

Online safety is taught progressively through the curriculum and reinforced through assemblies, pastoral provision, PSHE/RSE, computing and age-appropriate opportunities across the curriculum. Teaching reflects the four broad areas of online risk: content, contact, conduct and commerce.

- Children learn how to recognise unsafe, harmful, manipulative or inappropriate content and how to report it.
- Children learn about respectful online communication, cyberbullying, consent, privacy and digital footprints.
- Children learn how to protect accounts and personal information, including the importance of strong passwords and not sharing credentials.
- Children are taught to question information, images and online claims and understand misinformation and manipulated media.
- Children are taught age-appropriate risks associated with gaming, livestreaming, influencers, advertising, in-app purchases and online financial scams.
- Children receive age-appropriate education about online sexual harassment, sexual content, exploitation, grooming and image-sharing, in line with safeguarding and RSE provision.
- Children are taught about artificial intelligence, including safe, responsible and honest use and the risks of inaccurate, biased or harmful AI-generated content.
- Children with SEND and pupils with additional vulnerabilities receive reasonable adjustments and targeted support where required.

Filtering and monitoring

The school will maintain filtering and monitoring arrangements that meet current DfE expectations. Filtering is preventative; monitoring is reactive. Neither replaces effective supervision, professional judgement or safeguarding procedures.

- The Governing Body retains strategic responsibility and receives regular assurance.
- A named SLT lead, DSL and responsible governor will have clearly defined responsibilities.
- Filtering and monitoring will be reviewed at least annually and additionally after significant safeguarding incidents, changes in technology, network configuration, working practices or introduction of new services including generative AI.
- The review will consider pupils' age, SEND, EAL, safeguarding profile, curriculum needs, BYOD arrangements, remote access, apps, AI tools and known technical limitations.
- Filtering will block illegal, harmful and inappropriate content without unreasonably restricting legitimate teaching and learning.

- Filtering providers should use relevant IWF and CTIRU blocklists and maintain appropriate protections against users overriding them.
- Safe search will be enabled and appropriately secured.
- Filtering and monitoring will apply to school-managed devices and relevant school networks, including devices used off-site where technically applicable.
- Technical monitoring will provide weekly reports of incidents and immediate escalation for high-risk safeguarding, malicious or technical concerns, with appropriate identification of users/devices.
- All users will be informed that monitoring is in place.
- Monitoring data will be handled proportionately, securely and in accordance with data-protection requirements.
- Testing logs will record the date, person completing the check, what was tested and actions arising.
- Temporary exceptions to filtering will require appropriate SLT authorisation and documentation.
- Where filtering/monitoring identifies a safeguarding concern, the matter will be passed promptly to the DSL and managed under safeguarding procedures.

Responding to online safety incidents

Any member of staff who becomes aware of a concern should:

1. Stay calm and listen; do not promise confidentiality.
2. Do not investigate beyond what is necessary to establish immediate safeguarding information.
3. Preserve relevant evidence where safe to do so and avoid forwarding harmful material unnecessarily.
4. Report the concern immediately to the DSL or deputy DSL using the school's safeguarding reporting process.
5. Record the concern factually, including what was seen/heard, when, where and any immediate action taken.
6. Where there is immediate risk of harm, follow the school's emergency safeguarding procedures and contact emergency services where appropriate.

Incidents may include cyberbullying, grooming, exploitation, sexual abuse or harassment, harmful sexual behaviour, extremist content, self-harm content, threats, hate-related abuse, scams, hacking, malware, inappropriate images, impersonation, doxxing, non-consensual image sharing or serious breaches of school systems.

Cyberbullying and harmful online behaviour

Online bullying is treated as seriously as offline bullying. The school's Behaviour and Anti-Bullying policies apply. The school will consider the impact on the victim, the context, the age and vulnerability of pupils, the extent of the behaviour and whether safeguarding thresholds are met.

Digital images, video and consent

- Staff must follow school procedures for photography and video and use school-approved equipment/accounts wherever possible.
- Images of pupils must be stored securely and only used for legitimate educational, safeguarding or communication purposes.

- Staff must not post identifiable images of pupils on personal social-media accounts.
- Consent and privacy arrangements must be respected; however, safeguarding requirements take precedence where necessary.
- Pupils are taught that they must not photograph, record or share others without appropriate permission and must never share intimate or harmful images.

Social media and online communication

Staff must maintain professional boundaries online. Personal social-media accounts must not be used to communicate with pupils. Staff must not accept inappropriate contact requests from pupils or engage in private online relationships with pupils. School communication must use approved platforms and accounts.

Email, passwords and account security

- Passwords must be strong, unique and kept confidential.
- Staff must not share passwords or accounts unless explicitly authorised for a defined technical reason.
- Multi-factor authentication should be used where available and appropriate.
- Suspicious emails, links, attachments or requests for credentials must be reported.
- Staff must lock screens or log out when leaving devices unattended.
- School data must only be stored or transferred using approved systems.
- Any suspected account compromise must be reported immediately.
- Staff and Governors at AKPS receive annual training in Cyber Security

Artificial intelligence and emerging technology

Generative AI and emerging technologies may support teaching, administration and professional learning where their use is approved, proportionate and safe. The school will assess safeguarding, privacy, accuracy, bias, intellectual property and age-appropriateness risks before introducing new AI tools.

- Pupils must not enter personal, confidential or safeguarding information into public AI systems.
- Staff must not enter identifiable pupil information, safeguarding information or confidential school information into unapproved AI tools.
- AI-generated material must be checked for accuracy and suitability before use.
- Children will be taught that AI can produce inaccurate, biased, misleading or inappropriate content.
- Where AI is used to support assessment, planning or communication, professional judgement remains with the member of staff.
- AI use will be reflected in filtering/monitoring reviews and data-protection impact assessments where required.

Personal devices and mobile phones

Personal devices must be used in accordance with the school's Mobile Phone and Acceptable Use arrangements. Staff must not use personal devices to store or share pupil images or confidential information unless explicitly authorised under school procedures.

Remote learning and home use

Where learning takes place remotely, safeguarding expectations continue to apply. School-approved platforms should be used. Staff should maintain professional boundaries, use appropriate supervision and avoid unnecessary one-to-one private communication with pupils.

Data protection and privacy

Online safety measures must comply with UK GDPR and the Data Protection Act 2018. The school will process monitoring, filtering and safeguarding information lawfully, fairly and proportionately. Appropriate privacy information, retention arrangements, access controls and Data Protection Impact Assessments will be used where required.

Cyber security

- The school will maintain appropriate technical safeguards, updates, access controls, backups and malware protection.
- Staff must follow the school's cyber-security procedures and report suspected phishing, malware, data loss or unauthorised access immediately.
- Access rights will be reviewed and removed promptly when no longer required.
- School systems should be maintained in accordance with current DfE cyber-security standards and relevant National Cyber Security Centre guidance.

Vulnerable pupils and SEND

The school recognises that some pupils may be at increased risk online because of age, SEND, communication needs, social circumstances, mental health and wellbeing, exploitation risk or other safeguarding factors. Online safety teaching, filtering, monitoring and pastoral support will be adapted accordingly and considered within individual safeguarding and support plans where appropriate.

Parents and carers

The school will provide parents/carers with age-appropriate advice about online safety, parental controls, social media, gaming, privacy, scams and reporting routes. Parents/carers are encouraged to talk regularly with children about their online lives and to contact the school where online activity is affecting a child's safety, wellbeing or education.

Staff training and awareness

Online safety forms part of safeguarding induction and ongoing training. Staff will be updated on emerging threats, filtering and monitoring procedures, AI, cyber security, online abuse and reporting arrangements. Staff must understand how their role contributes to online safeguarding.

Monitoring, assurance and review

- The DSL will review relevant online safeguarding concerns and filtering/monitoring reports.

- Filtering and monitoring effectiveness will be formally reviewed at least annually and after significant changes or incidents.
- The responsible governor will receive assurance that the school is meeting its online safety responsibilities.
- The school will maintain records of testing, incidents, actions and outcomes.
- Policy effectiveness will be reviewed annually, or earlier when guidance, technology, legislation or local safeguarding risks change.

Acceptable Use – core pupil expectations

- I use technology safely, respectfully and responsibly.
- I keep my passwords and personal information private.
- I tell an adult if I see something online that worries or upsets me.
- I do not bully, threaten, embarrass or exclude others online.
- I ask permission before taking or sharing photographs or recordings.
- I do not meet online contacts in person without a trusted adult's involvement.
- I do not buy, download or install things without permission.
- I understand that online actions can have real-world consequences.
- I use AI only in ways that my teacher or school has said are safe and appropriate.

Staff quick-response flow

SEE / HEAR concern → STOP and ensure immediate safety.

REPORT → DSL / deputy DSL immediately.

RECORD → factual safeguarding record using school procedures.

ESCALATE → DSL considers referral to children's social care, police, Prevent or other agency where thresholds are met.

TECHNICAL ACTION → IT/appropriate lead addresses account, device, filtering or security issue.

REVIEW → record outcome and consider whether teaching, supervision, filtering, training or policy needs strengthening.

Policy review checklist

- ☐ KCSIE 2026 requirements checked Yes
- ☐ DfE filtering and monitoring standard checked Yes
- ☐ Annual filtering/monitoring review completed Yes
- ☐ Responsible SLT lead identified Yes Mr Dan Hockaday, Deputy Head
- ☐ Responsible governor identified Yes Michele Collier Bromelow (nominated safeguarding governor)

- ☐ DSL responsibilities confirmed Yes
- ☐ IT provider responsibilities documented Yes
- ☐ Weekly monitoring reports operational Yes Oakford notifications
- ☐ High-risk alerts have an immediate response route yes SWGFL and Oakford
- ☐ SafeSearch and appropriate blocklists confirmed yes
- ☐ AI tools and risks reviewed yes
- ☐ DPIA/privacy arrangements checked
- ☐ Staff online-safety training completed yes and annual cyber training of staff and Governors
- ☐ Pupil online-safety curriculum reviewed yes
- ☐ Parent information reviewed yes on website
- ☐ Incident and testing logs reviewed
- ☐ Related policies cross-referenced and consistent yes

Appendix 1 – Key current 2026 reference points

KCSIE 2026 came into force on 1 September 2026. The DfE filtering and monitoring core standard was updated on 16 September 2026 and includes requirements concerning governance, annual review, filtering, monitoring, AI-generated content, safe search, reporting and incident response. Ofsted's state-funded school inspection toolkit applies from September 2026 and includes expectations that pupils are taught how to stay safe online and that school information systems safeguard pupils effectively from online harm.