



ARK AEP Online Safety Policy-September 2026

Policy owner: Designated Safeguarding Lead – Kay Walton/ Senior Leadership Team

Applies to: All pupils, staff, volunteers, trustees/governors, visitors, contractors and partner providers

Review cycle: At least annually and following any significant online safety incident, technology change or statutory update

Statutory context: This policy is written in line with Keeping children safe in education 2026, which sets out the safeguarding duties schools and colleges in England must follow, including online safety as part of a whole-school safeguarding approach.

1. Purpose and principles

ARK AEP is committed to safeguarding and promoting the welfare of all children and young people, including when they are online. Online safety is not a standalone technical issue; it is an integral part of safeguarding, behaviour, curriculum, pastoral care, attendance, data protection and staff conduct. This policy provides a clear framework for preventing, identifying and responding to online risks while enabling pupils to benefit from technology safely and responsibly.

All adults working with or on behalf of ARK AEP must adopt a child-centred approach, act in the best interests of the child, and follow safeguarding procedures promptly where concerns arise. This reflects the expectation in KCSIE 2026 Part One that safeguarding is everyone's responsibility and that all staff understand and discharge their roles.

2. Scope

This policy applies to the use of all digital technology connected with ARK AEP, including school-owned devices, personal devices used for school purposes, internet access, cloud services, communication platforms, learning platforms, cameras, social media, messaging services, artificial intelligence tools, remote education systems and any technology used on or off site where it may affect pupil safety, wellbeing, learning or the reputation of the provision.

3. Roles and responsibilities

- **Proprietor:** ensure that online safety is embedded within safeguarding governance, that appropriate filtering and monitoring systems are in place, and that effectiveness is reviewed at least annually.
- **Leaders of ARK AEP Provision:** ensures that this policy is implemented, resourced, communicated and reviewed, and that online safety incidents are managed consistently.
- **Designated Safeguarding Lead:** takes lead responsibility for online safety within safeguarding practice, supports staff to identify and respond to online harms, and works with leaders and IT support on filtering and monitoring arrangements.
- **Senior leader responsible for filtering and monitoring:** oversees filtering and monitoring arrangements and leads the annual effectiveness review with support from the DSL and technical support.
- **IT support / service provider:** implements and maintains technical controls, supports testing, provides reports and responds promptly to safeguarding-related technical issues.
- **All staff and volunteers:** follow this policy, report concerns immediately, model safe digital behaviour and complete required safeguarding and online safety training.
- **Pupils:** are expected to use technology safely, responsibly and respectfully, in line with behaviour expectations and acceptable use rules.
- **Parents and carers:** are encouraged to work in partnership with ARK AEP to promote safe and responsible technology use.

4. Online safety risks

ARK AEP recognises that children may experience online risks both inside and outside school. These include contact risks, conduct risks, content risks and commerce-related risks. In line with KCSIE 2026, staff must be alert to harmful online content and behaviour, including bullying, grooming, exploitation, sexual harassment, radicalisation, serious

violence, misinformation, disinformation, conspiracy theories, harmful challenges, image-based abuse, deepfake or AI-generated abuse, self-harm content, illegal content, scams and coercive behaviour.

5. Filtering and monitoring

ARK AEP will maintain appropriate filtering and monitoring systems to reduce the risk of pupils accessing harmful or inappropriate content through school systems. These arrangements will be proportionate to pupil needs, age, vulnerability, curriculum requirements and the nature of alternative education provision. In line with KCSIE 2026 and sector guidance, ARK AEP will review the effectiveness of filtering and monitoring systems at least once every academic year, keep records of checks and actions, and ensure that leadership, safeguarding and technical staff are involved in the review.

- Filtering will be tested across school-managed devices, relevant networks and key locations.
- Monitoring alerts and reports will be reviewed by appropriate staff and escalated where safeguarding concerns are identified.
- Any weaknesses, over-blocking or under-blocking will be recorded and addressed promptly.
- Staff will know how to report concerns about filtering, monitoring or pupil access to harmful content.
- The DSL will be informed of online safety patterns, recurring concerns and significant incidents.

6. Education and curriculum

ARK AEP will teach pupils how to stay safe online through the curriculum, pastoral work, assemblies, targeted interventions and day-to-day conversations. Online safety education will be age-appropriate, trauma-informed and responsive to pupils' needs. It will include privacy, consent, respectful communication, digital footprints, online relationships, reporting concerns, critical evaluation of information, misinformation and disinformation, cyberbullying, exploitation, harmful content, AI-generated content and safe use of devices and platforms.

7. Acceptable use of technology

All users must use ARK AEP technology lawfully, safely and respectfully. Users must not access, create, store, share or distribute illegal, harmful, abusive, discriminatory, extremist, sexually explicit, violent or otherwise inappropriate material. Users must not attempt to bypass filtering or monitoring, share passwords, impersonate others, misuse

images, record others without permission, or use technology to bully, intimidate, exploit or harass.

8. Mobile phones and personal devices

ARK AEP will manage mobile phones and personal devices in line with safeguarding, behaviour and learning expectations. Pupils may only use personal devices where this has been explicitly authorised by staff. Unauthorised use, recording, image-sharing, messaging, hotspotting or attempts to access blocked content will be managed through behaviour and safeguarding procedures. Staff must use school-approved systems for professional communication and must not use personal accounts or personal devices to contact pupils unless this is explicitly authorised as part of an agreed safeguarding plan.

9. Artificial intelligence and emerging technologies

ARK AEP recognises that artificial intelligence and emerging technologies can support learning but may also create safeguarding risks, including deepfake content, image manipulation, impersonation, misinformation, automated grooming, plagiarism, misuse of pupil data and harmful recommendations. Staff must not upload personal, sensitive or confidential pupil information to AI tools unless the tool has been approved for that purpose and data protection requirements have been met. Any concern involving AI-generated or manipulated content must be treated as a safeguarding concern and reported to the DSL.

10. Reporting and responding to concerns

All online safety concerns must be reported without delay in line with ARK AEP safeguarding procedures. Staff must record concerns accurately, preserve relevant evidence where safe and appropriate, and avoid investigating beyond their role. The DSL will assess concerns, consider immediate safety needs, involve parents or carers where appropriate, contact external agencies when required, and ensure that support is provided to any pupil affected.

Where online concerns involve suspected crime, child sexual exploitation, child criminal exploitation, radicalisation, harassment, sharing of nude or semi-nude images, threats of serious harm, coercion, blackmail or significant welfare concerns, the DSL will follow statutory guidance, local safeguarding partnership procedures and, where necessary, seek advice from children's social care, the police or other relevant agencies.

11. Staff conduct and professional boundaries

Staff must maintain professional boundaries online and must follow ARK AEP's staff code of conduct, safeguarding policy and acceptable use requirements. Staff must not communicate with pupils through personal social media, personal messaging accounts or unapproved platforms. Any accidental contact, inappropriate communication or concern about another adult's online conduct must be reported immediately in line with allegation and low-level concern procedures.

12. Remote learning and off-site provision

Where pupils access remote learning, alternative provision, outreach support or off-site digital learning, ARK AEP will ensure that safeguarding arrangements remain clear. Staff must use approved platforms, maintain professional standards, consider pupil vulnerability, report concerns promptly and ensure that any partner provider understands and follows agreed safeguarding and online safety expectations.

13. Data protection, privacy and records

ARK AEP will process personal data lawfully, fairly and securely. Images, recordings, monitoring data, safeguarding records and online incident records must be handled in line with data protection law, confidentiality expectations and safeguarding record-keeping procedures. Staff must only use approved systems for storing and sharing pupil information and must report any suspected data breach promptly.

14. Training and awareness

All staff will receive safeguarding training that includes online safety, filtering and monitoring responsibilities, reporting routes, professional conduct, AI-related risks and the needs of vulnerable pupils. Governors, trustees, leaders, volunteers and relevant partner providers will receive information appropriate to their roles. Pupils and parents or carers will be supported through accessible guidance, curriculum opportunities and communication about emerging online risks.

15. Monitoring, evaluation and review

This policy will be reviewed at least annually by the DSL, senior leadership and the proprietor, trustees or governing body. The review will consider statutory updates, local safeguarding priorities, incident records, pupil voice, staff feedback, filtering and monitoring checks, technology changes and lessons learned. Any urgent changes required to protect pupils will be implemented without waiting for the annual review date.

Review on- 1.9.27

Created by – Kay Walton