



ONLINE SAFETY POLICY

Last Review Date	September 2026
Policy Reviewer	Director – Kane Wilson
Version	V2 22/9/26
Changes since last review	-
Next Review Date	September 2027
Applies to	All staff, volunteers, learners, visitors/contractors where relevant

1. PURPOSE AND STATUS

This policy sets out how The Ark keeps children safe when internet access, Wi-Fi, computers, tablets, mobile phones, smart devices, cameras, messaging, social media, generative artificial intelligence (AI) or other digital technology are used during a placement or affect safeguarding at the provision.

The policy is deliberately proportionate to The Ark's limited technology use. It does not assume that The Ark operates the same digital infrastructure or curriculum as a large school. Where KCSIE 2026 or DfE digital standards place duties directly on schools and colleges, commissioning schools retain those duties. The Ark nevertheless adopts those standards as safeguarding good practice for the systems and activities it controls and as part of Leeds commissioning assurance.

2. LEGAL AND GUIDANCE FRAMEWORK

- Keeping Children Safe in Education 2026 (KCSIE) – statutory guidance for schools and colleges; used by The Ark as the principal safeguarding benchmark.
- Working Together to Safeguard Children 2026.
- DfE Alternative Provision guidance and the Non-school Alternative Provision: Voluntary National Standards.
- DfE Filtering and Monitoring Core Standard and related digital/cyber-security standards.
- DfE Generative Artificial Intelligence (AI) in Education guidance and Generative AI Product Safety Standards.
- DfE Mobile Phones in Schools 2026 – directly applicable to schools; adopted by The Ark proportionately as good practice.
- UK GDPR and Data Protection Act 2018; Equality Act 2010; Computer Misuse Act 1990; Online Safety Act 2023 where relevant to service providers.

- Leeds Safeguarding Children Partnership (LSCP), Leeds for Learning Education Safeguarding and relevant West Yorkshire safeguarding procedures.
- UKCIS guidance on sharing nudes and semi-nudes, SWGfL and Internet Watch Foundation guidance/resources.

3. ROLES AND RESPONSIBILITIES

DIRECTOR

- has overall strategic responsibility for this policy and for proportionate online-safety controls on Ark-managed systems;
- ensures responsibilities for filtering, monitoring, cyber security, device management and escalation are assigned and understood;
- receives assurance that filtering/monitoring controls are operating as intended and that the annual effectiveness review is completed and recorded;
- ensures contracts or technical support arrangements permit prompt correction of weaknesses.

DESIGNATED SAFEGUARDING LEAD (DSL)

- leads on online safeguarding concerns and ensures online risk is considered alongside offline risk;
- reviews safeguarding alerts/incidents, decides next safeguarding steps and liaises with commissioning schools, parents/carers and statutory agencies as appropriate;
- contributes to the annual filtering/monitoring effectiveness review and to decisions about emerging technology and AI;
- ensures trends, repeated concerns and individual vulnerabilities inform risk assessment and safeguarding planning.

ALL STAFF AND VOLUNTEERS

- follow this policy, the Safeguarding & Child Protection Policy and Staff Code of Conduct;
- provide active supervision when learners use digital devices;
- report harmful content, suspicious contact, device misuse, filtering weaknesses or other online safeguarding concerns to the DSL without delay;
- never investigate a safeguarding concern beyond what is necessary to establish immediate safety and make a clear report.

4. ONLINE RISK FRAMEWORK – THE 4CS

The Ark considers online risk through the four overlapping areas used in KCSIE:

RISK AREA	EXAMPLES RELEVANT TO SAFEGUARDING
Content	Exposure to illegal, inappropriate, misleading or harmful material, including child sexual abuse material, pornography, violent material, extremist content, racism, misogyny/misandry, hate, self-harm, suicide or eating-dis-

RISK AREA	EXAMPLES RELEVANT TO SAFEGUARDING
	order content, harmful challenges, misinformation, disinformation and conspiracy material, including AI-generated content.
Contact	Harmful interaction with other people or systems, including grooming, coercion, sexual or criminal exploitation, scams, unknown adults, unsafe online relationships, impersonation, social-media contact and interaction with conversational or companion-style AI systems.
Conduct	A child's or adult's online behaviour that creates or increases harm, including cyberbullying, harassment, abusive or discriminatory messages, location sharing, livestreaming, sexual harassment, harmful sexual behaviour, making/sending/receiving nudes or semi-nudes, and creation or distribution of AI-generated or manipulated images/deep-fakes.
Commerce	Risks involving money or commercial influence, including gambling, inappropriate advertising, phishing, fraud, scams, in-app purchases and coercive or exploitative financial activity.

5. ACCESS TO TECHNOLOGY AT THE ARK

Technology is not the main mode of delivery at The Ark. Learners primarily participate in outdoor, animal-care and forest-school activities. Any learner internet/device use should therefore be limited, purposeful, supervised and linked to an agreed activity or individual need.

- Learners may only use Ark-managed internet access or devices with staff permission and appropriate supervision.
- Access to general web search, video platforms or other online services is staff-directed and not an entitlement.
- Personal devices do not become 'safe' merely because a pupil is on site. Mobile data may bypass Ark filtering and must be managed through the personal-device rules below.
- Any new learner-facing digital service, app or AI tool must be considered for safeguarding, privacy, age-appropriateness, SEND accessibility and data-protection risk before routine use.

6. FILTERING AND MONITORING

Where The Ark provides internet access or Ark-managed devices, it will maintain proportionate filtering and monitoring arrangements suited to its small scale, learner risk profile and actual technology use. These arrangements adopt the principles of the DfE Filtering and Monitoring Core Standard as safeguarding good practice.

FILTERING

- Filtering must be active and kept up to date on Ark-managed internet connections/devices where technically applicable.
- Controls should block illegal child sexual abuse material, unlawful terrorist content and adult content as a minimum, and should address other harmful content proportionately.
- The Ark will use a reputable filtering service/provider and will seek assurance that relevant IWF and counter-terrorism blocklists are implemented where the service provides this functionality.
- Any temporary exception to filtering must be authorised by the responsible Director and recorded.
- After new devices, services, AI tools or significant technical changes, The Ark will check that safeguards still operate as intended.

MONITORING

- In-person staff supervision is the primary monitoring control because learner device use is limited and supervised.
- Where technical monitoring or provider logs are available, these will be used proportionately to identify harmful or inappropriate activity.
- High-risk safeguarding concerns identified by any monitoring method must be passed to the DSL immediately.
- If a technical monitoring service is used, responsibilities for reviewing alerts/reports and escalating safeguarding concerns must be documented.

CHECKS AND ANNUAL EFFECTIVENESS REVIEW

- Routine checks will be proportionate to the technology in use and will confirm that intended filtering/security controls remain active.
- Checks will be logged with the date, person completing the check, what was tested, the result and any action taken.
- The Director, DSL and relevant technical support will complete a formal filtering/monitoring effectiveness review at least once each academic year, adopting the DfE school/college standard as good practice.
- The review will also be repeated or brought forward after a significant safeguarding incident, major network/device change, new BYOD arrangement, introduction of learner-facing generative AI, or a material change in risk.
- The review will consider learner age, SEND and communication needs, individual risk profile, mobile-data/BYOD risk, emerging harms, incidents/trends, what the filter blocks/allows, system limitations and whether controls cover all Ark-managed devices and relevant connections.

7. MOBILE PHONES, SMART DEVICES AND PERSONAL TECHNOLOGY

The Ark operates a mobile-device-free default during learner sessions. This is a proportionate safeguarding and engagement measure and reflects the direction of DfE statutory guidance for schools, while recognising that The Ark is a non-school AP.

- Pupil phones, smart watches and other personal connected devices should normally be switched off or placed in the agreed storage location at the start of a session and returned at the agreed time.

- A reasonable adjustment or exception may be agreed for medical, SEND, communication, travel or other safeguarding need. The reason and any controls should be clear.
- A pupil may use a personal device in an emergency when directed by staff.
- Use of personal mobile data to bypass Ark controls during sessions is not permitted.
- Pupils must not photograph, film, livestream or audio-record another pupil or member of staff without explicit permission.
- Pupils must not use personal devices to access social media, messaging, gaming or online communities during sessions unless this is specifically authorised for a safeguarding or educational purpose.
- Staff personal phones should normally be kept away from pupils and used only for legitimate work or emergency purposes in accordance with the Staff Code of Conduct.
- Staff must not use personal devices for private communication with pupils.

8. PHOTOGRAPHY, VIDEO AND AUDIO

- Photography or video may be used for learning records, activities, communication with commissioning schools, safeguarding records or publicity only where there is a clear lawful and safeguarding purpose.
- Consent and/or another appropriate lawful basis must be established as required by the Data Protection Policy and any placement/parental arrangements.
- Images should avoid unnecessary identifying information, precise location information or other details that increase risk.
- Ark-approved devices/accounts should be used wherever practicable. Staff must not retain pupil images on personal devices.
- If exceptional circumstances make temporary use of a personal device unavoidable for an immediate safeguarding purpose, the image must be transferred securely to the approved system as soon as possible and permanently deleted from the personal device/cloud backup, with the DSL informed.
- Images shared with commissioning schools must use approved secure channels.
- Images selected for website/social-media publication must be checked for consent, safeguarding suitability and unnecessary identification.
- Pupils may photograph animals or activities only with staff permission and must avoid capturing other pupils unless permission has been specifically given.

9. STAFF SOCIAL MEDIA AND ELECTRONIC COMMUNICATION

- Staff must maintain clear professional boundaries online and follow the Staff Code of Conduct.
- Staff must not add, follow or accept pupils on personal social-media accounts, or enter private online relationships with pupils except where an unavoidable pre-existing family relationship exists and has been declared where appropriate.
- Staff must not direct-message pupils through personal social media, WhatsApp, personal email or other private accounts.
- Communication with pupils, parents/carers and commissioning schools must use approved work channels wherever available.
- Staff must not post confidential information, pupil images, placement information or commentary about pupils/parents/colleagues on personal accounts.

- Online conduct outside work may be considered under safeguarding, low-level concern/allegation or disciplinary procedures where it raises a concern about suitability to work with children.

10. GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

AI can support some administrative or educational tasks, but it can also create safeguarding, privacy, misinformation, manipulation and image-abuse risks. AI use at The Ark must be purposeful, proportionate and subject to human professional judgement.

STAFF USE

- Staff must not upload identifiable or confidential pupil information, safeguarding records, EHCP information, photographs, health information or other sensitive personal data to public/general-purpose AI systems unless an approved arrangement, lawful basis and data-protection assessment expressly permit it.
- AI outputs must be checked for accuracy, bias, appropriateness and safeguarding risk before being used or shared.
- AI must not be used to make safeguarding decisions, risk assessments or referral decisions in place of the DSL or professional judgement.
- Staff must not use AI to create misleading, humiliating, sexualised or impersonating content involving pupils, colleagues or other identifiable people.
- Any AI product proposed for learner-facing use should be assessed for age/SEND suitability, filtering, monitoring, privacy, security and escalation features.

PUPIL USE

- Pupil use of generative AI is permitted only when specifically authorised and supervised.
- Learners must not enter personal or sensitive information about themselves or others into AI tools.
- Learners must not use AI to create sexual, violent, humiliating, hateful, bullying, impersonating or deceptive content.
- Learners should be reminded that AI can fabricate information and that outputs require checking.
- Use that creates a safeguarding concern will be dealt with under this policy and the Safeguarding & Child Protection Policy, not treated only as a behaviour issue.

11. NUDES, SEMI-NUDES, SEXUAL IMAGERY, SEXTORTION AND DEEPFAKES

Any nude or semi-nude image involving a person under 18, including self-generated, digitally altered, deepfake or wholly AI-generated sexual imagery, must be treated as a safeguarding concern. The same applies to sextortion, sexual coercion, image-based abuse and suspected child sexual abuse material.

- Staff must not unnecessarily view, open, copy, print, screenshot, forward, save, download or share sexual imagery involving children.
- Staff must not ask a child to send the image to them or to reproduce it.
- The concern must be reported immediately to the DSL, who will follow current KCSIE/UKCIS safeguarding guidance and consider the need for police, Children's Social Care or other specialist involvement.

- Where an image may constitute illegal child sexual abuse material, staff must avoid actions that create additional copies or distribution.
- The commissioning school will be informed promptly unless doing so would create a safeguarding risk or conflict with advice from statutory agencies.

12. RESPONDING TO ONLINE SAFEGUARDING INCIDENTS

When an online concern arises, staff should use the following sequence:

1. Protect immediate safety. Stop harmful access/contact where this can be done safely and support the child.
2. Do not conduct an unnecessary investigation. Listen, establish only the information needed to understand the immediate concern, and do not promise confidentiality.
3. Preserve relevant information without creating or distributing unnecessary copies. For sexual imagery, follow the stricter rules in section 11.
4. Report the concern to the DSL immediately or, if unavailable and there is urgent risk, follow the Safeguarding & Child Protection Policy escalation route.
5. Record the concern factually, including what happened, platform/device if known, action taken and who was informed.
6. The DSL assesses whether the matter is primarily safeguarding, child-on-child abuse, behaviour, staff conduct/allegation, potential criminality, or a combination.
7. Inform the commissioning school promptly in accordance with placement arrangements and safeguarding need.
8. Make or coordinate any referral to Children's Social Care, police, LADO or other service where required; urgent action is not delayed by uncertainty about which organisation should lead.
9. Consider parents/carers unless doing so may place the child at greater risk or conflict with statutory-agency advice.
10. Review whether individual risk assessment, support plan, attendance/missing-child arrangements, device rules, filtering/monitoring or placement arrangements need to change.

Online incidents outside The Ark are still safeguarding matters for The Ark where they affect a learner's safety, wellbeing, behaviour, attendance, relationships or risk while attending the provision.

13. SEND AND ADDITIONAL VULNERABILITY

Children attending alternative provision may be more vulnerable to grooming, exploitation, coercion, cyberbullying, unsafe online relationships, social isolation, misunderstanding boundaries and oversharing. The Ark will not assume that a child understands risk because a rule has been explained once.

- Online-safety explanations will be adapted to the learner's communication, cognitive, sensory and emotional needs.
- Reasonable adjustments may include visual prompts, repetition, simplified language, supported device routines or individually agreed exceptions.
- Responses to incidents will consider whether SEND or communication needs affected understanding, consent, disclosure or the child's ability to protect themselves.
- Individual risk assessments/support information provided by commissioning schools should identify relevant digital vulnerabilities where known.

14. STAFF TRAINING AND LEARNER EDUCATION

- Online safety is included in safeguarding induction for staff and volunteers.
- Staff receive safeguarding updates at least annually and additional updates when significant online risks, guidance or technology change.
- Training includes: current online harms; child sexual/criminal exploitation; harmful sexual behaviour; nudes/semi-nudes and AI/deepfake imagery; generative AI; filtering/monitoring responsibilities; mobile-device controls; and how to report concerns.
- Learner education at The Ark is proportionate and practical. Staff reinforce safe and respectful use when technology is used and provide direct support when an individual online risk is identified.
- Commissioning schools normally retain responsibility for the wider statutory curriculum, including RSHE and broader planned online-safety education.

15. SECURITY AND ACCEPTABLE USE

- Passwords must be strong, kept confidential and not shared.
- Staff must report suspected compromise, phishing, malware, unusual account activity or cyber-security weakness promptly.
- Unauthorised software, browser extensions or applications must not be installed on Ark-managed devices.
- Work information must be stored and shared using approved systems and in line with the Data Protection Policy.
- Learners must use Ark devices only for the purpose authorised by staff and must not attempt to bypass filtering, access another person's account, hack systems, install software or deliberately access harmful/illegal material.
- Where accidental access to harmful material occurs, the learner should close/stop access if safe to do so and tell a member of staff immediately; staff should record/report the issue proportionately.

16. GOVERNANCE, AUDIT AND REVIEW

- The Director owns the policy; the DSL leads on safeguarding content and incident response.
- The Director and DSL will review online-safety incidents for patterns, repeated platforms/content, individual vulnerabilities and control weaknesses.
- Filtering/monitoring check records and the annual effectiveness review will be retained as evidence for internal assurance and commissioning due diligence.
- The policy will be reviewed at least annually and earlier if KCSIE/DfE/Leeds guidance changes, significant new technology is introduced, or an incident shows that controls require amendment.
- Emerging risks such as new AI services, deepfake techniques, harmful online trends or new forms of exploitation will be incorporated into risk assessment, staff updates and learner support.

17. CROSS-POLICY LINKS

- Safeguarding & Child Protection Policy
- Staff Code of Conduct / Staff Behaviour and Safer Working Practice Policy
- Data Protection / GDPR Policy and Privacy Notice

- Positive Behaviour Policy
- Prevent arrangements and Prevent Risk Assessment
- Whistleblowing Policy
- Allegations / low-level concerns procedures
- Attendance / Missing Children Policy
- Photography / consent arrangements where held separately
- Business Continuity / cyber-security arrangements where relevant

APPENDIX A – LEARNER ACCEPTABLE-USE EXPECTATIONS

- I will follow staff instructions about phones, smart watches and other devices.
- I will only use The Ark's internet or devices when staff give permission.
- I will not try to bypass filters or security controls.
- I will not photograph, film, livestream or record another person without permission.
- I will not use technology to bully, threaten, humiliate, sexually harass, discriminate against or impersonate someone.
- I will not create, request or share nude/semi-nude, sexual or deepfake images.
- I will not share my location, passwords or other private information in ways that could put me or someone else at risk.
- I will tell staff if I see something upsetting, harmful, sexual, threatening or suspicious online, or if someone online makes me feel unsafe.
- If I accidentally access something harmful, I will stop and tell staff rather than hide it.
- I understand that The Ark may supervise or monitor use of its own devices and networks for safety and security.

APPENDIX B – FILTERING AND MONITORING CHECK RECORD

Date	Checked by	What was tested/checked	Result	Action / completion date

Suggested checks include: intended blocked categories, approved access, device coverage, new devices/services, user profiles, security updates, logs/alerts where used, mobile/BYOD risks and any reported weaknesses.

APPENDIX C – ANNUAL ONLINE-SAFETY / FILTERING AND MONITORING EFFECTIVENESS REVIEW

- What technology and internet access did learners actually use this year?
- Which Ark-managed devices and connections are covered by filtering/security controls?
- What is blocked/allowed, and does this remain proportionate to learner risk and legitimate use?
- How are personal mobile data and BYOD risks controlled?
- Are monitoring arrangements proportionate and do staff know how to report concerns?
- Were there any safeguarding incidents, repeated attempted access or emerging risks that require change?
- Do current arrangements consider SEND, communication needs and individual vulnerability?
- Have any generative-AI tools been introduced, and were they risk assessed?

- Are technical support contacts/responsibilities current and can weaknesses be corrected promptly?
- Were check records completed and actions closed?
- What changes are required to policy, training, devices, filtering, supervision or commissioner arrangements?

APPENDIX D – REFERENCE NOTE ON COMMISSIONING RESPONSIBILITY

Where a school commissions The Ark, the school continues to be responsible for safeguarding the pupil and for satisfying itself that the placement is safe and suitable. The Ark is responsible for safe practice within its provision, maintaining effective safeguarding arrangements, reporting incidents and sharing information promptly. The lead for a specific external referral should be agreed where possible, but safeguarding action must not be delayed where a child may be at risk.