



ALTERNATIVE ACRES

Online Safety and E-Safety Policy

Academic Year 2026/27

Policy owner	Head of Provision
Head of Provision	Gemma Robertson
DSL / Online Safeguarding Lead	Daun Beresford
Deputy DSL	Gemma Robertson
Approved by	Gemma Robertson
Date reviewed	01/09/2026
Next review	01/09/2027 or sooner if technology, risk or guidance changes

Online safety is part of safeguarding. Concerns about a child must be reported to the DSL and recorded on CPOMS in accordance with the Child Protection and Safeguarding Policy.



1. Purpose

Alternative Acres is committed to providing a safe digital and online environment for children and young people while helping them develop the knowledge, judgement and confidence to use technology safely.

Online safety is not limited to internet use at the provision. Harm can arise through social media, messaging, gaming, image sharing, artificial intelligence, live-streaming, online communities and other digital services, including when incidents take place away from Alternative Acres but affect a learner's safety or wellbeing.

This policy sets out expectations for learners, staff, volunteers, contractors and visitors and explains how Alternative Acres will prevent, identify, record and respond to online-safety concerns.

2. Status and guidance

Alternative Acres is a non-school alternative provision. Keeping Children Safe in Education 2026 and the Department for Education's digital technology standards are written for schools and colleges; Alternative Acres adopts relevant safeguarding principles as good practice and commissioner assurance while applying the legal and contractual requirements that are directly relevant to the provision.

This policy has been reviewed with reference to:

- Keeping Children Safe in Education 2026.
- Working Together to Safeguard Children 2026.
- DfE Filtering and Monitoring: Core Standard, updated 25 August 2026.
- DfE digital leadership, cyber security and device standards where relevant to the provision's technology.
- UK Council for Internet Safety guidance, including guidance on sharing nudes and semi-nudes.
- Prevent duty guidance and relevant data-protection legislation.

3. Scope

This policy applies to:

- All learners attending Alternative Acres.
- Employees, mentors, volunteers and agency staff.
- Contractors, visitors and external professionals where they use or have access to technology at the provision.
- Alternative Acres-owned or managed devices and accounts.
- Internet access provided or arranged by Alternative Acres.
- Remote or online activity undertaken on behalf of Alternative Acres.



- Online behaviour outside the provision where it creates a safeguarding concern, affects another learner or staff member, or has a direct impact on the safe operation of the provision.

4. The four areas of online risk

Alternative Acres uses the four-area model of online risk:

- Content - exposure to illegal, inappropriate or harmful material, including pornography, sexual content, violence, self-harm and suicide content, eating-disorder content, racism, misogyny, hate, extremism, misinformation, disinformation and harmful AI-generated material.
- Contact - harmful interaction with other people online, including grooming, coercion, exploitation, adults posing as children, peer pressure, stalking and unwanted contact.
- Conduct - a person's own online behaviour that creates or increases risk, including cyberbullying, harassment, sharing intimate images, oversharing personal information, abusive messaging and unsafe live-streaming.
- Commerce - risks such as scams, phishing, gambling, in-game purchases, financial exploitation, advertising and fraudulent schemes.

These risks can overlap. Staff should consider the wider context, including exploitation, domestic abuse, child-on-child abuse, radicalisation, criminal exploitation and mental-health risk.

5. Roles and responsibilities

5.1 Head of Provision

- Ensures that online safety is embedded in safeguarding, staff conduct, risk assessment and provision practice.
- Ensures resources and suitable technical support are obtained where needed.
- Ensures technology arrangements described in policy reflect what Alternative Acres actually uses.
- Ensures significant online-safety incidents are reviewed and lessons are implemented.

5.2 DSL / Online Safeguarding Lead

Daun Beresford, DSL, has lead safeguarding responsibility for online safety. The DSL will:

- Receive and respond to online safeguarding concerns.
- Ensure concerns about children are recorded on CPOMS.
- Coordinate referrals to children's social care, police, Prevent/Channel or other agencies where appropriate.
- Consider online safety within safeguarding training and learner support.
- Contribute to the review of filtering and monitoring arrangements and safeguarding risks.



5.3 Staff, volunteers and agency workers

- Model safe and professional technology use.
- Follow the Staff Code of Conduct, Mobile Phone and Smart Device Policy and approved communication arrangements.
- Supervise learner technology use according to individual need and risk.
- Report online-safety concerns immediately to the DSL.
- Do not investigate safeguarding concerns or search through a learner's device themselves.
- Complete online-safety training and updates relevant to their role.

5.4 Learners

- Use Alternative Acres technology only for agreed purposes.
- Follow staff instructions and acceptable-use expectations.
- Treat other people respectfully online.
- Tell a trusted adult if they see or experience something worrying, harmful or uncomfortable.
- Never deliberately bypass filtering, security or account controls.

6. Online safety education

Alternative Acres will provide online-safety education that is age, development and need appropriate. Teaching may be delivered through mentoring, PSHE/RSHE, Functional Skills activity, discussion of current events and individual safeguarding work.

Education will include, where appropriate:

- Privacy, passwords and personal information.
- Online friendships, grooming and exploitation.
- Cyberbullying and abusive behaviour.
- Consent and respectful communication.
- Sharing nudes and semi-nudes.
- Social media, gaming and live-streaming.
- Scams, gambling and financial risk.
- Extremist, hateful or manipulative content.
- Misinformation, disinformation, conspiracy material and source checking.
- Artificial intelligence, synthetic media and deepfakes.
- How to report content, block users and seek help.
- The impact of an online footprint and permanence of shared material.



7. SEND and additional vulnerability

Many learners at Alternative Acres have SEND, SEMH needs, anxiety, communication differences or other vulnerabilities that can affect how online risk is understood or experienced.

Staff will not assume that chronological age reflects online understanding. Support will be adapted to the individual learner and may include:

- Concrete language and visual explanations.
- Repeated teaching and rehearsal of safe responses.
- Support with recognising grooming, manipulation, coercion and scams.
- Explicit teaching about private/public information and boundaries.
- Individual safety planning with parents/carers and commissioners where appropriate.
- Consideration of how a learner's communication, social understanding, impulsivity or need for connection may increase online vulnerability.

8. Technology used at Alternative Acres

Alternative Acres will maintain an accurate understanding of the devices, accounts and connectivity that are actually used. Policy wording must not claim technical systems that cannot be evidenced.

Learner access to laptops and the internet at Alternative Acres is limited to educational purposes. Laptops are used for approved learning activity, including BKSb and other agreed educational resources.

Staff will direct learners to the websites, platforms and resources required for the planned educational activity and will remain present while the device is in use. Learners are not provided with unsupervised or open-ended internet access.

Learners are not left unattended with laptops or other Alternative Acres internet-connected devices. Their use is directly supervised by a member of staff at all times. The majority of learners attend on a one-to-one basis, with other learners supported in very small staffing arrangements. This high level of direct supervision forms an important part of Alternative Acres' online-safety controls, alongside proportionate technical filtering and monitoring.

9. Filtering and monitoring

Filtering and monitoring are important safeguards but do not replace supervision, education, professional curiosity or safeguarding reporting.

Alternative Acres will have filtering and monitoring arrangements that are appropriate and proportionate to the technology and internet access actually provided. The separate Filtering and Monitoring Policy/Procedure will



document the current technical arrangement and evidence. Because learners are directly supervised whenever they use laptops, and the laptops are used only for planned educational purposes, human supervision is a significant safeguarding control; it complements rather than replaces appropriate technical filtering and monitoring.

As an adopted safeguarding standard, Alternative Acres will:

- Identify who is responsible for filtering and monitoring decisions and safeguarding oversight.
- Understand what internet-connected devices and connections are in use and which are covered by filtering/monitoring.
- Use filtering capable of reducing access to harmful and inappropriate content without unnecessarily blocking legitimate learning.
- Use a monitoring approach proportionate to the level and type of learner access.
- Review effectiveness at least once each academic year and whenever technology or safeguarding risk changes.
- Check that controls operate as intended on relevant internet-connected devices and in relevant locations and retain a record of those checks.
- Understand and document limitations, including any device, connection, hotspot or service that falls outside central controls.
- Have a clear route for staff to report a filtering/monitoring concern or failure.

No filtering system can be assumed to be completely effective. Staff must continue to supervise learners and report concerns even where technical controls are in place.

10. Responding to unsuitable or harmful content

If a learner or member of staff encounters unsuitable content unexpectedly:

- Do not continue browsing, forwarding or sharing the material.
- Move away from or close the content where it is safe and appropriate to do so.
- Do not ask a child to show illegal sexual imagery to another adult.
- Report the incident to the DSL where there is a safeguarding concern.
- Record the child safeguarding concern on CPOMS where applicable.
- Preserve relevant information such as the URL, search term, time, device and account where this can be done without viewing, copying or storing illegal material.
- Report a suspected technical filtering failure through the provision's filtering/monitoring route.

Where content may be illegal, staff will follow DSL, police, Internet Watch Foundation or other appropriate agency advice and must not deliberately download, copy or redistribute it.



11. Artificial intelligence and generative AI

Alternative Acres recognises that generative AI tools can create educational opportunities as well as safeguarding, privacy, accuracy and integrity risks.

- Learners may only use generative AI where a member of staff has approved the specific activity and tool.
- Staff must assess whether a tool is suitable for the learner's age, needs, data protection and safeguarding context before use.
- Personal, confidential, safeguarding, health or identifiable learner information must not be entered into public generative AI systems unless there is an approved lawful arrangement.
- AI output must not be treated as automatically accurate or safe.
- Learners will be taught that AI can produce false, biased, manipulative or inappropriate content.
- Staff and learners must not use AI to create sexualised, humiliating, threatening or deceptive images/content of another person.
- Suspected AI-generated sexual imagery, deepfakes, grooming or harmful impersonation will be treated as a safeguarding concern.
- Filtering/monitoring reviews will consider emerging generative AI risks and whether approved or blocked services remain appropriate.

12. Social media, messaging and gaming

Learners are not permitted to use social media, personal messaging or gaming services during the provision day through personal devices or Alternative Acres equipment unless an explicitly approved educational activity requires a particular service.

Online incidents occurring outside provision hours may still require Alternative Acres safeguarding action where they:

- Involve or threaten harm to a learner.
- Constitute child-on-child abuse, sexual harassment, exploitation or bullying.
- Create a risk that continues into Alternative Acres.
- Involve an adult working with Alternative Acres.
- Require information sharing with parents/carers, commissioners, police or children's social care.

Staff must not contact learners through personal social-media accounts, personal messaging apps, gaming accounts or disappearing-message services.

13. Mobile phones and personal smart devices

Alternative Acres operates a zero-routine-use approach for learner mobile phones during the provision day.



- A learner may bring a phone where needed for travel or before/after provision.
- At the beginning of the day or session, the learner will be asked to switch the device off and place it in the designated secure storage arrangement.
- The phone remains securely stored for the provision day/session and is returned at the end.
- Learners do not routinely access phones during lessons, mentoring, breaks, lunch, animal care, practical work or outdoor activity.
- Urgent contact between a parent/carer and learner will be facilitated through Alternative Acres.
- A narrow exceptional adjustment may be agreed in advance by the Head of Provision/DSL for a genuine medical, accessibility, SEND or safeguarding need.
- A parent/carer request alone does not create an exception.
- Staff will not use physical force to obtain a phone. Refusal will be managed calmly and escalated to the Head of Provision/DSL, parent/carer and commissioner where appropriate.

Full arrangements are contained in the Mobile Phone and Smart Device Policy.

14. Staff personal devices and professional communication

Staff must maintain clear professional boundaries in all digital communication.

- Personal phones must not be used to photograph, video or audio-record learners.
- Personal social-media or messaging accounts must not be used to communicate with learners.
- Staff must not provide learners with personal mobile numbers, personal email addresses or personal social-media details.
- Where contact with parents/carers or learners is necessary, approved Alternative Acres channels must be used.
- Personal devices should be kept secure and should not distract from supervision, animal handling, driving or other safety-critical work.
- Any unavoidable emergency use of a personal device involving a learner must be reported and managed transparently.

15. Photography, video and audio

Images and recordings of learners will only be created for legitimate Alternative Acres purposes using approved equipment or accounts and in accordance with consent, safeguarding and data-protection arrangements.

- Staff must never use personal devices to create learner images or recordings.
- Learners' stored phones must not be used to photograph or record on site.
- Images must not be uploaded to personal accounts.



- Consent does not override safeguarding; an image must still be appropriate and safe to create, store and publish.
- Any suspected covert or sexualised recording must be reported immediately to the DSL.

16. Sharing nudes and semi-nudes

Sharing nudes and semi-nudes involving a person under 18 is a safeguarding matter. Staff must follow current UKCIS guidance and the Child Protection and Safeguarding Policy.

When a concern is reported, staff must:

- Report it to the DSL immediately.
- Never view, copy, print, forward, save or ask a child to download the image or video.
- If imagery has been viewed inadvertently, report this to the DSL immediately.
- Do not ask the child to delete material before the DSL has considered the correct safeguarding response.
- Do not blame, shame or interrogate the child.
- Do not conduct a search of the child's device.

The DSL will assess risk and consider referral to police and/or children's social care in line with current guidance and the circumstances of the case.

17. Online child-on-child abuse

Alternative Acres treats online child-on-child abuse as seriously as face-to-face abuse. It may include:

- Cyberbullying and discriminatory abuse.
- Sexual harassment or sexual violence with an online element.
- Threats, coercion or blackmail.
- Sharing intimate images without consent.
- Pressure to create or share sexual content.
- Abuse within teenage intimate relationships.
- Group chats used to isolate, humiliate or target a child.
- AI-generated sexualised or humiliating material.
- Hazing, threats or encouragement of offline violence.

The absence of a report does not mean abuse is not occurring. Staff must remain professionally curious and report concerns to the DSL.



18. Searching or examining learner devices

Alternative Acres staff must not rely on school-specific statutory search powers as though they automatically apply to this non-school alternative provision.

Staff should not search through a learner's personal phone or device, demand passwords, or inspect private content as an informal behaviour-management response.

Where a device may contain evidence of a safeguarding concern or criminal offence:

- Secure the situation without viewing or forwarding material unnecessarily.
- Inform the DSL immediately.
- Seek parent/carer, police, children's social care or other specialist advice as appropriate.
- Where necessary, preserve the device safely while advice is obtained.
- Do not intentionally view suspected indecent images of children.

The routine secure storage of a switched-off learner phone at the start of a session is not treated as a disciplinary confiscation.

19. Email, accounts and passwords

- Alternative Acres work accounts must be used for official communication.
- Passwords must not be shared with learners or unauthorised people.
- Users must lock or sign out of devices when leaving them unattended.
- Sensitive information must only be sent or shared through approved and appropriately secure systems.
- Phishing, suspicious links or account compromise must be reported promptly.
- Multi-factor authentication should be used where the relevant service supports it and it is proportionate to the account risk.
- Learners must not use another person's account or attempt to access restricted areas.

20. Remote or online learning

Any remote or online provision will be planned rather than improvised. Approved platforms/accounts will be used and staff will maintain the same safeguarding and professional-boundary expectations that apply on site.

- Staff must not conduct remote learning through personal social-media accounts.
- One-to-one remote sessions must be authorised and appropriately recorded/transparent.
- Parents/carers will be told what technology or platform is being used where appropriate.
- Staff will consider the learner's home context, SEND needs, privacy and ability to seek help.



- Any disclosure or safeguarding concern arising online must be handled under the Child Protection and Safeguarding Policy and recorded on CPOMS.

21. Parents, carers and commissioners

Alternative Acres will work with parents/carers and commissioners where online risk affects a learner's safety, access to education or placement.

- Parents/carers will be informed of significant online-safety incidents involving their child where appropriate.
- Alternative Acres will explain the provision's learner phone arrangements and approved technology use.
- Commissioners will be informed where an incident is serious, persistent, affects placement safety or requires coordinated safeguarding action.
- Information sharing will be proportionate and will prioritise safeguarding.

22. Online conduct by staff and allegations

Concerns about a member of staff's online behaviour will be dealt with under the Staff Code of Conduct and Managing Allegations and Low-Level Concerns Policy.

This includes personal communication with learners, inappropriate social-media interaction, misuse of images, sexualised online behaviour involving children, boundary breaches or online conduct suggesting that the adult may not be suitable to work with children.

Where the harm threshold may be met, the Head of Provision will use the appropriate LADO route. Concerns about the Head of Provision must be referred directly to the relevant LADO.

23. Recording and escalation

Where an online incident raises a child safeguarding concern, CPOMS is the principal and authoritative safeguarding record.

Records should include, as appropriate:

- What happened and how the concern came to attention.
- The child's own words where relevant.
- Platform/service/device involved.
- Known usernames, URLs or identifiers where safe and lawful to record.
- Immediate protective action.
- Advice or referrals sought.
- Decisions and rationale.



- Parent/carer and commissioner communication.
- Follow-up and outcome.

Staff must not copy illegal imagery into CPOMS or other records.

24. Training

Online safety will form part of safeguarding induction and ongoing staff updates. Training will reflect the technology actually used at Alternative Acres and the needs of its learners.

Training will include:

- The four areas of online risk.
- Online exploitation, grooming and child-on-child abuse.
- Professional communication and personal-device boundaries.
- Sharing nudes and semi-nudes.
- Artificial intelligence and deepfake/synthetic-media risks.
- Filtering and monitoring responsibilities appropriate to role.
- How to report technical failures and safeguarding concerns.
- The relationship between online safety, Prevent and SEND vulnerability.

25. Monitoring, review and quality assurance

The Head of Provision and DSL will review this policy at least annually and sooner where the provision's technology, connectivity, learner profile, incidents or national guidance changes.

Quality assurance will include:

- Review of online-safety incidents and CPOMS themes.
- Filtering and monitoring review and recorded technical checks.
- Device, account and internet-connection inventory.
- Staff training and policy acknowledgement.
- Review of generative AI and emerging online risks.
- Consistency with the Mobile Phone and Smart Device Policy.
- Any commissioner or safeguarding audit feedback.
- Lessons from incidents, attempted bypasses or filtering failures.

26. Related Alternative Acres policies

- Child Protection and Safeguarding Policy 2026/27



- Filtering and Monitoring Policy/Procedure
- Mobile Phone and Smart Device Policy
- Staff Code of Conduct 2026/27
- Managing Allegations and Low-Level Concerns Policy 2026/27
- Social Media Policy
- Remote Learning Policy
- Data Protection Policy
- Anti-Bullying Policy
- Behaviour Management Policy
- Prevent / safeguarding arrangements
- Staff Training and Induction Policy

Quick staff response guide

Learner sees harmful content	Stop/close safely, reassure, report to DSL if safeguarding-related and report any filtering failure.
Suspected nude/semi-nude image	Do not view, copy or forward. Tell DSL immediately.
Online bullying/exploitation/grooming	Tell DSL; record child safeguarding concern on CPOMS.
Filtering or monitoring appears not to work	Stop further learner access where necessary and report the technical/safeguarding issue promptly.
Concern about staff online conduct	Use Staff Code of Conduct / Managing Allegations and Low-Level Concerns route.
Immediate danger	Call 999 and take immediate protective action.

Policy approval

Approved by	Gemma Robertson
DSL	Daun Beresford
Date	07/09/2026
Next review	07/09/2027 or sooner if required