THE ALTERNATIVE SCHOOL GROUP LTD

Online Safety and Acceptable Use of ICT Policy

Author:	**HB**
Date:	**25th September 2026**
To be reviewed:	**July 2027**
Reviewed:	**Nov '16, Dec '17, May '18, Oct '19, Nov '19, Feb 20, May 21, Sept 21, May 22, Sept 22; Sept 24; July 25; Sept 26;**
Version:	**13**

Note: This policy has been developed and reviewed by The Alternative School Group Limited using internal expertise, professional judgement, current statutory guidance and appropriate digital tools. Final approval and responsibility for the policy rests with The Alternative School Group Limited.

© 2026 by The Alternative School Group Ltd. All rights reserved.

1. Purpose and Status

The Alternative School Group Ltd (TAS) recognises that safeguarding children includes safeguarding them online. Technology is integral to education and administration, but it can also facilitate harm. This policy establishes a whole-school approach to protecting and educating pupils, supporting staff and parents/carers, and identifying, intervening in and escalating online-safety concerns.

It should be read with the Safeguarding and Child Protection Policy, Staff Code of Conduct, Relationships, Responsibility and Community Policy, Anti-Bullying/Cyberbullying arrangements, Data Protection Policy, Social Media Policy, Remote Learning arrangements and the separate Staff ICT Acceptable Use Policy. The latest statutory requirement takes precedence if guidance changes before this policy is formally reviewed.

2. Statutory and Guidance Context

Framework / guidance	Policy response
Keeping Children Safe in Education 2026	Online safeguarding, staff responsibilities, DSL oversight, filtering and monitoring.
DfE Filtering and Monitoring: Core Standard (September 2026)	Defined roles; risk-based provision; annual documented review; safeguarding reporting; dynamic and AI-generated content.
EYFS statutory framework for group and school-based providers (September 2026)	Safeguarding, screen use and devices with imaging/sharing capability.
UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025	Lawful, transparent and secure processing; accountability and privacy information.
DfE generative AI guidance and product safety standards	Risk assessment, age restrictions, safeguarding, data protection, human oversight and accuracy.
Prevent duty guidance	Protection from online radicalisation and extremist content.
Current ISI / Ofsted inspection framework as applicable	Evidence that safeguarding arrangements are effective in practice and regularly reviewed.

3. Governance, Leadership and Responsibilities

- The proprietor has overall responsibility for ensuring effective safeguarding arrangements, including appropriate online-safety, filtering and monitoring arrangements.
- The Headteacher/BSS ensures this policy is implemented, resourced, understood and reviewed.
- The Designated Safeguarding Lead (DSL) takes lead responsibility for online-safety safeguarding concerns and works closely with IT support.
- IT support is responsible for secure operation of systems and for supporting filtering, monitoring, cyber-security and authorised incident investigation.
- All staff and volunteers must understand the school's online-safety expectations, complete required training, supervise pupils appropriately and report safeguarding concerns promptly to the DSL/DDSL.
- Pupils are taught to use technology safely, respectfully, responsibly and critically and to report concerns.
- Parents/carers are supported with information about online risks and encouraged to reinforce safe and responsible use.

© 2026 by The Alternative School Group Ltd. All rights reserved.

4. Online-Safety Risks

Content: illegal, harmful or inappropriate material; pornography; violence; self-harm or suicide content; hate; extremism; misinformation/disinformation; harmful challenges; gambling; body-image content; and AI-generated or manipulated material.

Contact: grooming, exploitation, coercion, harassment, radicalisation, unwanted contact, scams, impersonation and contact with adults or peers who may pose a risk.

Conduct: cyberbullying, abusive/discriminatory behaviour, sharing intimate images, sexual harassment, oversharing, unsafe digital footprints, plagiarism, copyright infringement and misuse of AI.

Commerce: online gambling, inappropriate advertising, phishing, financial scams, in-app purchases and risks involving money or personal/financial information.

5. Education and Curriculum

- Online safety is embedded across the curriculum, PSHE/RSHE and day-to-day technology use, appropriate to age, development, SEND, communication needs and vulnerabilities.
- Teaching includes privacy, passwords, consent, respectful communication, cyberbullying, scams, misinformation, copyright, digital reputation, healthy technology use, reporting routes and age-appropriate understanding of AI.
- Pupils are taught that filtering is not a substitute for safe decision-making and to tell a trusted adult if something online worries, frightens, pressures or confuses them.
- Staff reinforce safe online behaviour whenever technology is used and receive safeguarding training that includes online safety.

6. Filtering and Monitoring

TAS will maintain filtering and monitoring arrangements appropriate to its pupils, curriculum, devices and risk profile. Filtering and monitoring are separate but complementary safeguarding controls. No system is assumed to be 100% effective.

- The school will identify role-holders for strategic responsibility, DSL safeguarding oversight and technical management.
- Filtering will seek to block illegal and harmful/inappropriate content without unreasonably restricting teaching and learning.
- Monitoring arrangements will enable relevant concerns arising from pupil device/activity data to be identified, reviewed and escalated to the DSL in a timely way.
- The school will consider mobile/app content, off-site use of managed devices, encrypted services, real-time/dynamic content and AI-generated content when determining controls.
- Temporary filtering exceptions must be authorised, appropriately time-limited, documented and reviewed.
- At least annually, BSS, the DSL, IT support and the responsible proprietor/governance representative will review provision, risks, gaps, incidents and actions. The review and actions will be recorded and retained for inspection.
- Filtering and monitoring will also be reviewed following a serious incident, material technology change or change in pupil risk profile.
- Access to monitoring data and alerts is restricted to authorised staff with appropriate safeguarding and data-protection awareness.

TAS will maintain detailed operational arrangements, including current filtering and monitoring systems, testing, technical responsibilities, annual review records and associated actions in the

© 2026 by The Alternative School Group Ltd. All rights reserved.

schools ICT and Digital Technology Procedures and Systems Register. Passwords, PINs, recovery information and other credentials must never be included in this policy.

7. Generative Artificial Intelligence (AI)

- Only AI tools approved by TAS may be used for school business or pupil-facing activity.
- Staff must comply with product age restrictions and ensure pupil use is appropriately supervised and supported by suitable safety, filtering and monitoring controls.
- Personal, special-category, safeguarding, medical or other confidential information must not be entered into public or unapproved AI tools. Proposed use involving personal data must be discussed with the DPO/data-protection lead.
- AI outputs must be critically checked for accuracy, bias, safeguarding concerns, appropriateness and intellectual-property issues. Professional responsibility remains with the staff member.
- Pupils must be taught when AI use is permitted, how to acknowledge it where required, and that presenting AI-generated work as their own may constitute academic misconduct.
- AI-generated or manipulated sexual imagery, deepfakes, impersonation, harmful content or use of AI to bully, exploit, groom or deceive must be treated as safeguarding concerns and escalated to the DSL.
- New AI products or materially new uses will be risk assessed before adoption, considering safeguarding, data protection, security, age suitability and supplier/product safety information.

8. Data Protection, Privacy and Cyber Security

- Personal data will be processed in accordance with UK GDPR and the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025 and the school's Data Protection Policy.
- The school will provide appropriate privacy information about relevant monitoring and technology use, including what is monitored, why, who may access reports/alerts and applicable retention arrangements.
- A data protection impact assessment (DPIA) will be completed where required before introducing new high-risk technology, including new or materially changed filtering/monitoring or AI processing.
- School information must be stored and shared only through approved secure systems. Staff must report suspected phishing, malware, account compromise, data loss or data breach promptly.
- Passwords must be strong and unique; multi-factor authentication will be used where required or appropriate. Devices must be locked when unattended and kept updated.

9. Staff Use of Technology and Communications

- Staff must use official school accounts/systems for communication with pupils and parents/carers and maintain professional boundaries.
- Staff must not use personal social-media accounts or personal messaging channels to communicate with pupils except under an explicitly authorised emergency arrangement.
- Staff must not accept or initiate social-media connections with current pupils. Exceptional pre-existing relationships must be declared and managed under the Staff Code of Conduct.
- School business must not be conducted through personal email accounts.
- Staff must not attempt to bypass filtering, monitoring, security controls or device-management restrictions.
- Any illegal, inappropriate, harmful or safeguarding-related online material or incident must be reported immediately to the DSL/DDSL; technical faults should also be reported to IT.
- Personal-device use for school purposes must comply with the Staff ICT Acceptable Use Policy and data-protection requirements.

9A. Home and Remote Working

© 2026 by The Alternative School Group Ltd. All rights reserved.

This section applies when TAS has authorised remote work under its medical-related Work from Home Policy or another lawful, individually agreed arrangement. It does not create a general entitlement to home working. All security and safeguarding controls below remain mandatory for any authorised remote access.

The following requirements apply whenever staff undertake TAS business from home or another authorised remote location. They supplement the Data Protection Policy, Staff ICT Acceptable Use Policy and TAS Work from Home Policy.

- Where TAS provides or requires use of managed equipment, staff must use it in accordance with TAS policies and take reasonable steps to protect it from loss, theft, damage and unauthorised access.
- Only TAS-approved systems, software, applications, cloud storage and communication services may be used for TAS business where approval is required. TAS information must not be transferred to personal email accounts, personal cloud-storage accounts, unauthorised messaging services, unauthorised USB/removable media or other unauthorised equipment.
- Family members and other unauthorised people must not be permitted to use TAS equipment or access TAS accounts, systems or information.
- Staff must keep passwords and authentication credentials confidential, use multi-factor authentication where provided or required, lock devices when unattended and follow TAS requirements for secure remote access, including any approved VPN or equivalent solution.
- Staff must take reasonable steps to ensure that the network used for home working is secure. Confidential or personal information must not be accessed over unsecured public Wi-Fi unless an approved secure connection method is being used.
- Screens, paper records and confidential conversations must, so far as reasonably practicable, be protected from being seen or overheard by household members or other unauthorised people. Headphones or another private location should be used where appropriate.
- Printing confidential, safeguarding, commercially sensitive or personal information at home should be avoided unless there is a genuine business need. Any such material must be stored securely and must not be placed in ordinary household waste or recycling where this could disclose confidential or personal information; it should be returned for secure disposal where appropriate.
- TAS information should be stored only in approved locations. Staff should not retain local copies where an approved TAS network or cloud location is available and should comply with access controls and retention requirements.
- Any actual or suspected loss of TAS equipment or documents, misdirected information, phishing, malware, account compromise, unauthorised access, accidental disclosure or other data/security incident must be reported immediately through the relevant TAS reporting route. Staff must not delay reporting while attempting to resolve the incident themselves.
- All TAS equipment, records and information remain TAS property and must be returned or securely dealt with when requested or when employment ends. Staff must not retain copies of TAS information without authorisation.

Cross-reference: TAS Work from Home Policy.

10. Images, Video and Audio

- Images/video/audio of pupils may only be created for an authorised school purpose and in accordance with safeguarding, data-protection and consent arrangements.

© 2026 by The Alternative School Group Ltd. All rights reserved.

- Personal devices must not be used to photograph, film or record pupils unless an exceptional use has been expressly authorised under school policy.
- Images must be transferred promptly to approved secure school storage and removed from the capture device where appropriate.
- External publication will follow consent/privacy arrangements and will not unnecessarily identify pupils.

11. EYFS: Screen Use and Devices

Where TAS provides EYFS provision:

- Practitioners will have regard to children's screen use. It will be purposeful, proportionate and developmentally appropriate and will not displace high-quality adult interaction, play, movement, communication or direct experiences.
- Screens used for business or educational purposes must comply with safeguarding, data-protection and security requirements.
- The number of photographs/videos taken of children, including for assessment, will be kept to the minimum necessary and sharing with parents/carers will use technically secure approved methods.
- Safeguarding arrangements cover mobile phones, cameras and other electronic devices with imaging and sharing capabilities.
- Children will be discouraged from bringing personal devices into the setting; any exception will be managed with parents/carers and subject to safeguarding controls.

11A. Evergreen Forest Nursery – EYFS Online Safety Arrangements

Evergreen Forest Nursery follows the TAS safeguarding, online-safety and data-protection requirements. These additional arrangements apply to its EYFS provision.

- **Screen use:** Technology will be used purposefully, proportionately and under suitable adult supervision. It must not routinely replace play, outdoor learning, movement or direct interaction with practitioners.
- **Staff devices**: Personal phones, smartwatches, cameras and other image-capable devices must be managed under nursery procedures. Staff must not use personal devices to photograph or record children except where expressly authorised under TAS safeguarding procedures.
- **Photographs and recordings**: Images of children may only be created for authorised nursery purposes in line with safeguarding, privacy and relevant permission arrangements. Use TAS-approved devices and secure storage. Do not transfer images to personal accounts, personal cloud storage or unauthorised social media.
- **Parents and visitors**: Nursery will communicate rules on personal devices, photography and recording. Unauthorised recording or sharing of images of other children is not permitted.
- **Children's records**: Nursery information must be stored and shared through approved TAS systems, with any suspected loss or disclosure reported through the relevant safeguarding and data-protection procedures.
- **Digital platforms**: Nursery does not currently use an online learning journal or dedicated parent communication app. Any future system must be approved by TAS and assessed for safeguarding, data-protection and security risks before introduction.
- **Reporting and responsibilities**: Concerns about digital content, devices, unauthorised recordings or disclosure of children's information must be reported promptly to the DSL/DDSL and, where appropriate, the IT/data-protection lead. The Nursery Manager will ensure staff understand these requirements.

12. Mobile Phones and Pupil-Owned Devices

© 2026 by The Alternative School Group Ltd. All rights reserved.

TAS will maintain clear rules on pupil mobile phones and personal devices consistent with statutory guidance applying from September 2026 and with reasonable adjustments or exceptional arrangements required for individual pupils. Any permitted pupil-owned device remains subject to this policy, supervision and safeguarding controls.

13. Remote Learning and Online Communication

- Only school-approved platforms and accounts will be used.
- Professional standards, safeguarding expectations and acceptable-use rules apply equally to remote activity.
- Staff will consider privacy, background/environment, recording, access controls, invitations/links and the presence of other household members.
- Any recording must have a clear purpose, appropriate lawful basis/permission, secure storage and retention arrangement.
- Concerns arising during remote learning must be reported through normal safeguarding procedures.

14. Responding to Online-Safety Incidents

- A person encountering concerning content should stop where safe to do so, avoid unnecessary copying/sharing, preserve relevant evidence appropriately and report the concern.
- Safeguarding concerns are reported to the DSL/DDSL without delay. Immediate danger is managed under emergency procedures.
- The DSL determines safeguarding action, referrals and whether external agencies should be involved, including children's social care, police, Prevent/Channel, CEOP or the Internet Watch Foundation as appropriate.
- Incidents, decisions and actions will be recorded in school safeguarding/incident systems and shared only on a need-to-know basis.
- Technical action may include blocking, account suspension, device isolation, password reset, preservation of logs and review of filtering/monitoring controls.
- The school will consider whether an incident reveals a wider training, curriculum, policy or technical-control issue.

15. Pupil Acceptable-Use Principles

- I will use school technology for learning and authorised purposes.
- I will keep passwords private and will not use another person's account.
- I will be kind, respectful and responsible when communicating online.
- I will not deliberately search for, create, access or share illegal, harmful or inappropriate material.
- I will not try to bypass school filtering, monitoring, security or device restrictions.
- I will protect my own and other people's personal information.
- I will tell a member of staff if something online worries me, pressures me, seems unsafe or if I receive an upsetting message.
- I will only take, use or share images/recordings with permission and for an authorised purpose.
- I will respect copyright, acknowledge sources and follow school rules on the use of AI.
- I understand that school systems and managed devices may be filtered and monitored for safeguarding, security and appropriate-use purposes.

16. Review, Assurance and Inspection Evidence

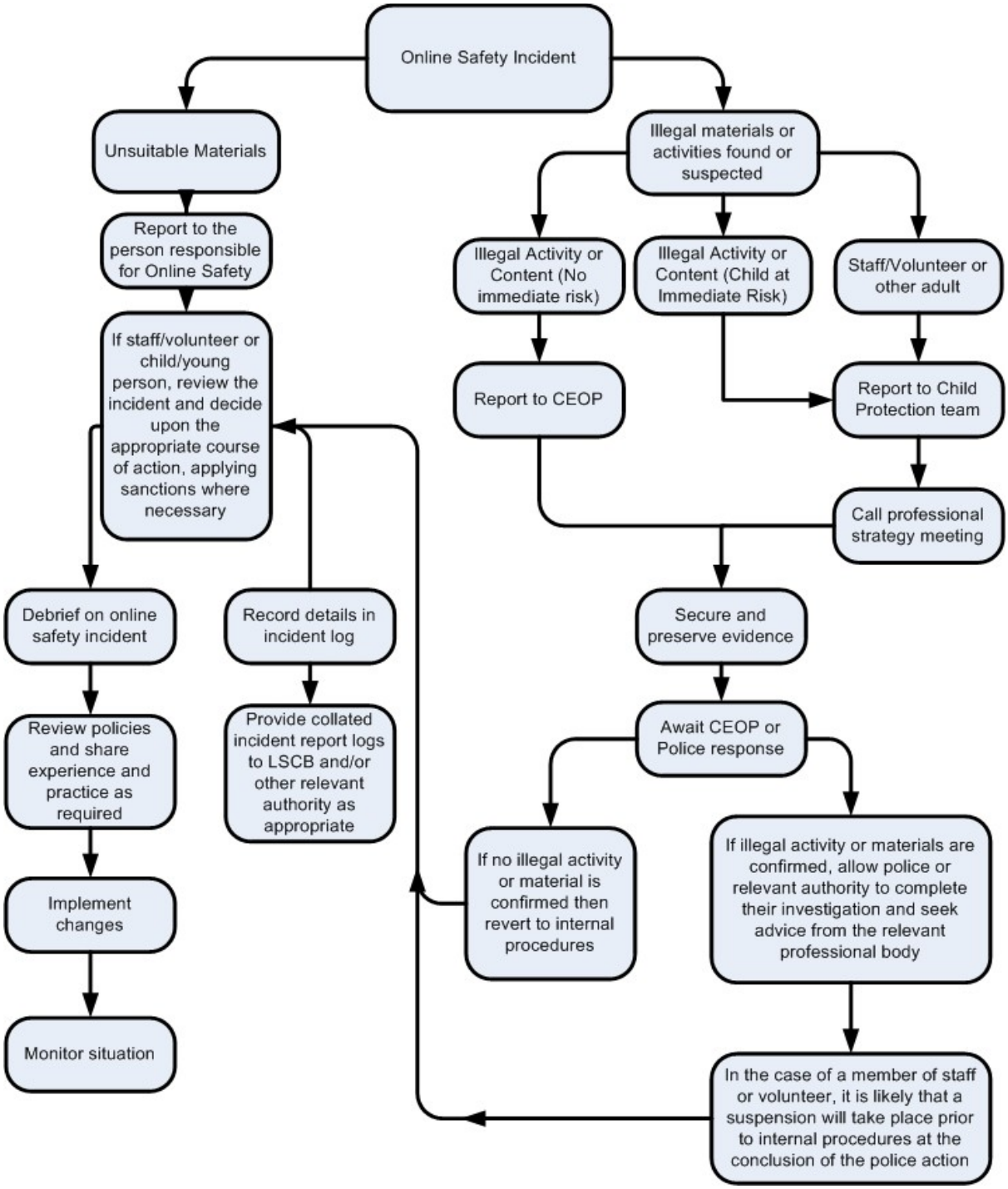
- This policy will be reviewed at least annually and sooner after significant statutory/guidance changes, technology changes or serious incidents.

© 2026 by The Alternative School Group Ltd. All rights reserved.

- Leaders will retain evidence that the policy operates in practice, including staff training, pupil education, incident records, filtering/monitoring reviews and tests, risk assessments, relevant DPIAs, technical assurance and actions arising.
- The proprietor/leadership will assure itself that practice across all campuses/settings is consistent with this policy.

Appendix A – Responding to Incidents of Misuse – Flow chart

© 2026 by The Alternative School Group Ltd. All rights reserved.



Source: South West Grid for Learning, 360º Safe

© 2026 by The Alternative School Group Ltd. All rights reserved.

Appendix B – Annual Filtering and Monitoring Review Record

Review date: _____

Participants (SLT / DSL / IT / proprietor or governance representative):

_____

Systems/services reviewed: _____

Pupil/staff risk profile considered:

_____

Current filtering: strengths/limitations:

_____

Current monitoring: strengths/limitations:

_____

Managed/off-site/mobile/app coverage:

_____

AI/dynamic content risk considered:

_____

Incidents/trends considered: _____

Testing undertaken and results:

_____

Actions, owner and deadline: _____

Date actions checked: _____

© 2026 by The Alternative School Group Ltd. All rights reserved.

Learn
Progress
Achieve
Success

© 2026 by The Alternative School Group Ltd. All rights reserved.

© 2026 by The Alternative School Group Ltd. All rights reserved.