



Online safety policy

Approved by:
The Directors of Strive Alternative Provision

Signed on behalf of the Directors by:
Stacey Hickey, Head of Operations

Date Approved: October 2026
Review Date: October 2027

Policy Update Summary (2026)

- Full review and rewrite for Strive Alternative Provision.
- Updated from Keeping Children Safe in Education 2023 to Keeping Children Safe in Education 2026.
- Updated filtering and monitoring arrangements to reflect the Department for Education's current digital and technology standards.
- Added current expectations for generative AI, deepfakes, synthetic media, data protection and safe use of AI tools.
- Strengthened arrangements for personal devices, BYOD, social media, online sexual harassment, sharing of nudes and semi-nudes, cyberbullying, scams, radicalisation and online exploitation.
- Clarified safeguarding reporting, staff responsibilities, filtering/monitoring review and incident response.

1. Purpose

Online safety is an integral part of safeguarding at Strive Alternative Provision. Technology provides valuable opportunities for learning, communication and preparation for adulthood, but it can also expose children and adults to harm. This policy sets out how Strive will promote safe, responsible and appropriate use of technology while responding promptly to online safeguarding concerns.

Strive is a commissioned alternative provision provider rather than a maintained school. Where statutory responsibilities sit with a commissioning school or local authority, Strive will cooperate with the commissioner and share relevant information. Strive will nevertheless maintain proportionate online-safety arrangements for the services, devices, networks and sessions it controls.

2. Scope

This policy applies to:

- All students attending Strive, including during off-site, outreach and community-based provision.
- Employees, directors, contractors, subcontractors, agency staff, volunteers and visitors.
- Strive-owned devices, networks, accounts and systems.
- Personal devices used for Strive purposes under authorised BYOD arrangements.
- Online conduct occurring away from Strive where it creates a safeguarding concern or materially affects a student, member of staff or the safe operation of provision.

3. Legal and Guidance Framework

This policy is informed by current legislation and guidance, including:

- Keeping Children Safe in Education 2026.

- Working Together to Safeguard Children 2026.
- DfE filtering and monitoring core standard within Meeting digital and technology standards in schools and colleges (updated 2026).
- Prevent duty guidance: England and Wales (2023).
- Online Safety Act 2023, where relevant to services used by Strive.
- UK GDPR and Data Protection Act 2018.
- Computer Misuse Act 1990.
- Equality Act 2010.
- DfE guidance on generative artificial intelligence in education and generative AI product safety standards.

4. The Four Areas of Online Risk

Strive recognises the four broad areas of online risk identified in safeguarding guidance:

- Content - exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm or suicide content, misinformation, radicalisation and extremist material.
- Contact - harmful interaction with others, including grooming, exploitation, coercion, peer pressure, impersonation and adults posing as children or young people.
- Conduct - behaviour that causes or increases the likelihood of harm, including cyberbullying, abusive messages, sexual harassment, creation or sharing of nudes or semi-nudes, and harmful use of images or recordings.
- Commerce - risks including scams, phishing, financial exploitation, inappropriate advertising and gambling-related content.

Online and offline harm frequently overlap. A child may experience abuse face to face and through digital channels at the same time, and children can abuse other children online.

5. Roles and Responsibilities

5.1 Directors and Senior Leadership

- Promote a culture in which online safety is treated as a safeguarding responsibility.
- Ensure proportionate arrangements exist for filtering, monitoring, cyber security and safe use of technology.
- Ensure online-safety arrangements are reviewed at least annually and following significant incidents or changes in technology or risk.
- Ensure staff understand how to report online safeguarding concerns.

5.2 Designated Safeguarding Leads

- Take lead responsibility for online safeguarding concerns and ensure appropriate action, recording, referral and information sharing.
- Understand the filtering and monitoring arrangements relevant to Strive's systems and sites.

- Consider online dimensions when assessing safeguarding concerns, including exploitation, child-on-child abuse, radicalisation, self-harm and sexual harm.

5.3 Head of Operations

- Coordinate implementation of this policy and work with IT providers, site partners and senior leaders on appropriate technical and operational controls.
- Ensure relevant incidents, weaknesses and actions are followed up.
- Ensure staff expectations for devices, accounts, passwords, data and communications are clear.

5.4 All Staff and Contractors

- Use technology professionally and in accordance with Strive policies and safeguarding expectations.
- Maintain professional boundaries online and never use personal social-media relationships to communicate with students.
- Report online safeguarding concerns to a DSL without delay.
- Never investigate a safeguarding concern themselves by searching for, downloading, forwarding or unnecessarily viewing illegal or harmful material.
- Protect passwords and accounts and report suspected compromise, phishing or data breaches promptly.

6. Filtering and Monitoring

Strive will take proportionate steps to ensure internet access and technology used within its control are appropriately filtered and monitored for the age, vulnerability and needs of its students. Filtering must seek to block harmful and inappropriate content without unreasonably restricting legitimate teaching and learning.

- Roles and responsibilities for filtering and monitoring will be identified.
- Arrangements will be reviewed at least annually and when there is a significant change in risk, technology, provider or site arrangements.
- Limitations of filtering and monitoring systems will be understood; no technical system is treated as a substitute for staff supervision, professional curiosity or safeguarding practice.
- Where Strive operates from shared or third-party premises, it will establish what filtering and monitoring arrangements are provided by the host and address any identified gaps proportionately.
- Concerns or alerts indicating possible safeguarding risk will be passed promptly to a DSL.

Staff must not deliberately disable, bypass or attempt to circumvent authorised filtering, monitoring or security controls unless this forms part of an approved technical support activity.

7. Personal Devices and BYOD

Personal devices may only be used for Strive purposes where authorised and in accordance with Strive's BYOD and data-protection arrangements. The fact that a device is personally owned does not remove professional, safeguarding or confidentiality obligations.

- Staff must not store student photographs, safeguarding information or other sensitive personal data on personal devices unless specifically authorised and appropriately protected.
- Personal messaging accounts and personal social-media accounts must not be used to form private relationships with students.
- Students' use of phones, smart watches and other personal devices may be restricted during sessions where necessary for safety, safeguarding, learning or individual risk management.
- Any search, confiscation or examination of a student's device must be lawful, proportionate and undertaken in accordance with Strive procedures and the circumstances of the concern.

8. Social Media, Messaging and Digital Communication

- Official or authorised channels should be used for communication relating to Strive business.
- Staff must maintain professional boundaries and appropriate privacy settings on personal accounts.
- Staff must not post confidential information, student information or images obtained through their work without lawful authority.
- Screenshots, disappearing messages and private groups do not remove professional accountability.
- Online harassment, discriminatory abuse, threats, impersonation or cyberbullying affecting the Strive community will be addressed under safeguarding, behaviour, HR or complaints procedures as appropriate.

9. Sharing Nudes and Semi-Nudes, Sexual Harm and Image-Based Abuse

Any incident involving the creation, possession, request, coercion, sharing or threatened sharing of nude or semi-nude images of a child must be treated as a safeguarding matter and referred immediately to a DSL.

- Staff must not ask a child to send, copy, print, forward or display an image for the purpose of investigating the concern.
- Staff must not save or share such imagery except where specifically directed by police or another competent safeguarding authority.
- The DSL will consider the child's immediate safety, coercion, exploitation, age and vulnerability, whether adults are involved, and whether referral to children's social care or police is required.

- AI-generated or manipulated sexual images of a child, including deepfakes, will be treated as a serious safeguarding concern.

10. Generative AI and Emerging Technology

Generative AI can support education and administration but may also create safeguarding, privacy, intellectual-property, bias, misinformation and accuracy risks. Use of AI must therefore be purposeful, proportionate and subject to professional judgement.

- Staff remain responsible for checking the accuracy, appropriateness and safety of any AI-generated content they use.
- Confidential, safeguarding, special-category or identifiable student information must not be entered into public or unapproved AI tools.
- Student-facing AI tools should only be used where their suitability, age appropriateness, privacy arrangements and safeguarding controls have been considered.
- Students should be taught that AI-generated information may be inaccurate or fabricated and should not be assumed to be factual.
- AI must not be used to create, manipulate or distribute abusive, sexualised, humiliating or deceptive content about another person.
- Suspected AI-generated harmful content, impersonation or deepfakes will be managed under the same safeguarding principles as other harmful online content.

11. Online Radicalisation and Extremism

Staff must be alert to online content, contact or behaviour that may indicate susceptibility to radicalisation or extremist influence. Concerns must be reported to a DSL in accordance with Strive's safeguarding and Prevent arrangements. Staff must not undertake their own investigation into extremist material.

12. Online Exploitation, Scams and Financial Harm

Online exploitation may include sexual exploitation, criminal exploitation, grooming, sextortion, coercion, scams, money-mule activity, phishing, gaming-related exploitation and financial abuse. Staff should remain alert to unexplained changes in behaviour, online contacts, gifts, money, devices or accounts and report safeguarding concerns promptly.

13. Photography, Video and Recordings

- Images and recordings of students must only be taken for legitimate Strive purposes and in accordance with consent, safeguarding and data-protection arrangements.
- Authorised Strive equipment or systems should be used wherever practicable.
- Images must not be posted to personal accounts or retained for personal use.
- Particular care must be taken where a child's location, identity, safeguarding status or family circumstances could create additional risk.

14. Responding to Online Safety Incidents

Where an online-safety concern arises, staff should:

- Prioritise immediate safety and report safeguarding concerns to a DSL.
- Preserve relevant evidence without unnecessarily viewing, copying or redistributing harmful material.
- Record the concern accurately on the appropriate Strive system.
- Follow data-breach, cyber-security, behaviour, complaints or HR procedures where these are also engaged.
- Inform parents/carers and commissioning organisations where appropriate and safe to do so.
- Contact police, children's social care or other agencies where required through safeguarding procedures.

If illegal content is suspected, staff should not search for or deliberately access further material. Advice should be sought from the DSL and, where necessary, police or another appropriate authority.

15. Education and Student Awareness

Online safety will be reinforced through day-to-day practice, PSHE, individual support and relevant curriculum activity. Students will be supported to understand privacy, consent, respectful communication, scams, misinformation, healthy technology use, reporting concerns and how to seek help.

Teaching and support will be adapted to students' age, developmental level, communication needs, SEND and individual vulnerabilities.

16. Staff Training

Online safety will form part of safeguarding induction and ongoing safeguarding updates. Relevant staff will receive additional information or training where technology, emerging risks, filtering and monitoring arrangements or individual student needs make this necessary.

17. Data Protection and Cyber Security

- Personal data must only be accessed, used and shared for legitimate purposes and through appropriate systems.
- Staff must use strong passwords and multi-factor authentication where available or required.
- Suspicious emails, links, attachments, account activity or suspected security incidents must be reported promptly.
- Devices must be locked when unattended and software/security updates must not be deliberately disabled.
- Any suspected personal-data breach must be managed under Strive's data-protection arrangements.

18. Monitoring and Review

The Head of Operations, DSL team and senior leaders will review relevant incidents, safeguarding themes, technical arrangements and emerging online risks. This policy will be reviewed annually, or sooner following significant changes to legislation, statutory guidance, technology, commissioning arrangements or Strive's operating model.

19. Related Policies

- Safeguarding & Child Protection Policy
- Anti-Bullying & Cyber-Bullying Policy
- Behaviour Management Policy
- GDPR & Data Protection Policy
- Staff Code of Conduct
- Whistleblowing Policy
- Anti-discrimination, Equality & Inclusion Policy
- Attendance & Engagement Policy
- BYOD / Acceptable Use arrangements

END OF POLICY

Version Control: 2026.1 | October 2026 | Full review and rewrite | Approved by Directors of Strive Alternative Provision