

Title	Online Safety Policy
Cross References	External: • DFE Filtering and Monitoring Core Standard (update June 2026) • DFE Generative AI in Education Guidance • DFE Generative AI Product Safety Standards • Keeping Children safe in Education 2026 • Data Protection Act 2018 and UK GDPR • Online Safety Act 2023 Internal: • Anti-Bullying Policy • Child Protection and Safeguarding Policy • Staff Code of Conduct • Data Protection and Privacy Policy • Acceptable Use Arrangements • Behaviour and Attendance Policy • Managing Allegations Against Staff Members Policy • Whistleblowing Policy
Date	October 2026

1. Policy Statement

Apricot Online Ltd is an online alternative education provider. Technology is not an additional element of our provision: it is the environment through which our teaching, communication, assessment and much of our safeguarding activity take place. Online safety is therefore integral to safeguarding, teaching and learning, data protection, professional conduct and organisational risk management.

Apricot Online is committed to enabling children and young people to benefit from digital technology while reducing their exposure to illegal, inappropriate and harmful content, contact, conduct and commercial risks. We recognise that no technical or educational control can remove all risk and that students often access Apricot provision from homes, personal devices and networks which Apricot does not own or control.

This policy is designed specifically for Apricot Online's remote model and should be read alongside the Child Protection and Safeguarding Policy.

2. Purpose

This policy sets out how Apricot Online will:

- provide a safe and secure online learning environment;
- define responsibilities for online safety across the organisation;
- manage risks arising from live online teaching, digital communication and remote access;
- apply appropriate filtering and monitoring to Apricot-controlled systems and understand the limits of those controls;
- support students to become safe, responsible and resilient digital users;
- manage risks arising from social media, online grooming, cyberbullying, sexual imagery, scams, misinformation and emerging technologies;
- set expectations for the safe use of generative artificial intelligence (AI);
- protect personal data, accounts, systems and digital content;
- respond promptly to online-safety incidents and safeguarding concerns; and
- work with parents/carers, commissioners, IT providers and other agencies where appropriate.

3. Scope

This policy applies to all staff, students, contractors and other authorised users of Apricot Online systems, learning platforms and communication channels. It also applies to online behaviour outside Apricot systems where that behaviour creates a safeguarding concern, affects another member of the Apricot community, compromises Apricot systems or data, or has a clear connection with Apricot provision.

The policy applies whether users access Apricot services through an Apricot-managed device, a commissioner-provided device or a personal/home device.

4. The Online Safety Risk Framework

Apricot Online uses the four broad areas of online risk identified in safeguarding guidance:

- Content - being exposed to illegal, inappropriate or harmful material, including pornography, self-harm or suicide content, extremist material, hate, violence, misinformation and disinformation.
- Contact - being subjected to harmful online interaction, including grooming, exploitation, coercion, harassment, stalking, scams or unwanted contact.
- Conduct - personal online behaviour that increases risk or causes harm, including bullying, sharing intimate images, abusive communication, impersonation, oversharing and unsafe use of technology.
- Commerce - risks including online gambling, inappropriate advertising, phishing, financial scams and other commercial exploitation.

Apricot Online also recognises risks created or amplified by artificial intelligence, deepfakes, synthetic media, algorithms, livestreaming, location sharing and rapidly changing digital services.

5. Roles and Responsibilities

5.1 Apricot Board and Senior Leadership

- Provide appropriate oversight of online-safety arrangements and organisational risk.
- Ensure online safety is considered within safeguarding, technology, data protection and curriculum decisions.
- Ensure staff have appropriate training and resources.
- Support proportionate technical controls and review arrangements appropriate to Apricot's online operating model.

5.2 Operations Director / Designated Safeguarding Lead

The Operations Director/DSL has lead operational responsibility for online safety where it intersects with safeguarding and is responsible for ensuring that online-safety concerns are assessed, recorded and escalated appropriately.

- maintain an up-to-date understanding of online safeguarding risks;
- ensure staff understand how to report online-safety concerns;
- review safeguarding themes arising from online incidents;
- liaise with commissioners, parents/carers, local authorities, police, LADO or other agencies where appropriate;
- ensure online-safety training is included within safeguarding development; and
- contribute to review of filtering, monitoring and emerging technology risks.

5.3 Managing Director, Department Heads and Managers

Managers are responsible for reinforcing this policy, supporting staff to use technology safely and professionally, escalating concerns and ensuring approved systems and processes are used within their areas.

5.4 IT Support / Managed Service Providers

IT support and managed service providers are responsible for implementing and maintaining agreed technical security, access, filtering and monitoring controls within the systems and devices that fall under Apricot's technical control, and for reporting relevant security or safeguarding concerns.

5.5 All Staff

- Use Apricot-approved systems and accounts for professional activity.
- Maintain secure passwords and account credentials and use multi-factor authentication where provided.
- Keep professional and personal online identities appropriately separate.
- Report safeguarding, security, data or online-safety concerns promptly.
- Maintain professional boundaries in all digital communication.
- Follow approved arrangements for live lessons, recordings, screen sharing, files and student data.
- Model safe and responsible technology use.
- Remain alert to emerging online risks and complete required training.

5.6 Students

Students are expected, according to their age, ability and individual needs, to use Apricot systems responsibly, protect account details, behave respectfully online, follow instructions designed to keep them safe and report anything that makes them feel unsafe, uncomfortable or worried.

5.7 Parents and Carers

Parents and carers play an important role because students commonly access Apricot provision through a home internet connection and a device outside Apricot's physical control. Apricot will provide or signpost appropriate information and will work with families where online-safety concerns affect a student's education or welfare.

6. Apricot's Online Learning Environment

Apricot Online uses approved digital platforms to deliver live teaching, learning resources, communication, assessment and student information. These include Google Workspace, Schoology and Adobe Connect, together with other systems approved by Apricot for specific organisational purposes.

- Users must access Apricot systems through their own authorised account.
- Login credentials must not be shared.
- Lesson links, meeting details and access credentials must not be shared with unauthorised people.
- Staff must use approved Apricot systems for communication with students.
- Staff must not move student communication to personal social-media accounts, personal messaging services or other unapproved channels.
- Unauthorised access, suspicious login activity or attempts to enter a virtual classroom must be reported.
- Staff must use professional language, content and conduct in all digital interactions.
- Personal devices may be used for work only in accordance with Apricot's security, confidentiality and data-protection requirements.

7. Live Online Lessons

Live online teaching creates particular safeguarding and online-safety considerations. Apricot's arrangements are designed around students and staff normally being in different physical locations.

- Virtual classrooms must use controlled access arrangements.
- Live lessons are recorded in accordance with Apricot's safeguarding, quality and data-protection arrangements.
- Recordings must be created and stored only through approved systems and must not be copied to personal devices.
- Authorised senior staff/DSLs may access live or recorded teaching where required for safeguarding, quality assurance or investigation.
- Staff should be alert to inappropriate messages, images, screen-shared material, usernames, links, background sounds, third-party interference or other indicators of risk.
- Where cameras are not used, staff must recognise that many visual indicators of harm will not be available and should remain attentive to voice, language, written communication, attendance and changes in behaviour.
- Screen sharing must be purposeful and managed carefully to avoid accidental disclosure of personal, confidential or inappropriate material.
- Students must not record, photograph, screenshot or redistribute lessons, staff or other students unless explicitly authorised.
- Where a lesson is disrupted by unauthorised access, abusive content or another online-safety incident, staff should secure the session where possible and report the incident promptly.

8. Filtering and Monitoring

Apricot Online recognises filtering as a preventative control designed to limit access to harmful or inappropriate content, and monitoring as a reactive control that can identify concerning user activity.

Because Apricot is a remote provider, the extent of technical control varies. Apricot can apply and manage controls within systems, accounts, services and devices for which it has administrative responsibility. Apricot cannot guarantee or directly manage the filtering or monitoring applied to a student's personal device, home broadband, mobile data connection or commissioner-controlled equipment.

Apricot will therefore:

- understand and document the coverage and limitations of its filtering and monitoring arrangements;
- apply appropriate controls to Apricot-managed systems and devices where technically available;
- ensure relevant users can be identified through authenticated accounts where possible;
- review technical arrangements and emerging risks at least annually and following significant change or incident;
- consider the age, SEND profile, vulnerability and online-learning needs of students when reviewing arrangements;
- work with commissioners where filtering or monitoring is their responsibility;
- ensure technical controls do not unreasonably restrict legitimate teaching and learning;
- maintain clear routes for staff to report content or activity that technical controls do not prevent; and
- consider whether systems can appropriately address dynamic, personalised and AI-generated content.

Technical filtering is not a substitute for safeguarding practice, staff vigilance, education, supervision and clear reporting routes.

9. Internet Searching and Learning Content

Students may need to use internet search tools and external websites as part of legitimate learning. Staff should select and check resources appropriately and provide greater guidance where the subject matter, student's age or vulnerability creates additional risk.

Some legitimate curriculum topics may involve sensitive material. Staff should plan these activities carefully and must not deliberately direct students to illegal or unnecessarily harmful content. Any requirement to adjust an Apricot-controlled technical restriction must be authorised, justified and auditable.

10. Social Media and Online Communities

Social media and online communities can support communication and creativity but can also expose children to grooming, exploitation, bullying, harassment, harmful content, impersonation and loss of privacy.

Students should be helped to understand:

- privacy settings and the limits of online privacy;
- the importance of strong passwords and account security;
- risks of sharing personal information, location and images;
- that online contacts may not be who they claim to be;
- how to block and report users or content;
- the permanence and potential reach of online posts;
- the need to seek permission before sharing images or information about others; and
- the importance of telling a trusted adult when something online causes concern.

Apricot staff must not befriend, follow or privately communicate with current students through personal social-media accounts. Staff use of social media must remain consistent with the Staff Code of Conduct and professional safeguarding expectations.

11. Cyberbullying, Harassment and Harmful Online Behaviour

Cyberbullying and online harassment may occur through messaging, social media, gaming, email, shared documents, images, video, impersonation or other digital services. Harm may occur outside Apricot's systems but still affect a student's safety, wellbeing or participation in provision.

Threatening, abusive, discriminatory, sexualised, humiliating or deliberately harmful online behaviour connected with Apricot provision will be addressed under safeguarding and/or behaviour procedures as appropriate.

Staff should preserve relevant evidence where safe and lawful to do so, record the concern and report it promptly. Staff must not download or circulate illegal sexual imagery of children.

12. Grooming, Exploitation and Harmful Contact

Online contact can be used to groom children for sexual abuse, criminal exploitation, radicalisation, financial exploitation or other harm. Grooming may occur gradually and may involve gifts, attention, secrecy, threats, coercion or moving a child to more private communication channels.

Any concern about grooming, exploitation or coercive online contact must be reported immediately to the DSL under the Child Protection and Safeguarding Policy.

13. Intimate Images, Sexual Content and Deepfakes

Concerns involving self-generated intimate images, non-consensual sharing of sexual imagery, sexual extortion, AI-generated sexual imagery or sexual deepfakes involving a child are safeguarding matters.

- Staff must not ask a child to forward or reproduce intimate imagery.
- Staff must not save illegal or intimate child imagery to a personal device.
- Where appropriate, staff may preserve non-illegal contextual evidence such as usernames, URLs, dates or written messages without unnecessarily viewing or copying sexual content.
- The DSL will assess and manage the concern in accordance with safeguarding procedures and seek specialist or statutory advice where required.

14. Generative Artificial Intelligence

Generative AI can support education but can also create safeguarding, accuracy, privacy, intellectual-property and academic-integrity risks. Apricot will take a proportionate, risk-based approach to AI use.

- Staff and students must follow any age restrictions and terms applying to an AI service.
- Student use of generative AI for Apricot learning should take place only where the tool and activity are considered appropriate and suitable safeguards are in place.
- Personal, confidential, safeguarding or special-category information must not be entered into public or unapproved AI tools.
- Users should understand that AI outputs can be inaccurate, biased, fabricated or manipulative and should not be treated automatically as reliable.
- AI-generated work should be acknowledged where required by Apricot or awarding-body expectations.
- AI must not be used to create, manipulate or distribute sexual, abusive, humiliating, discriminatory or deceptive material about another person.
- Staff selecting learner-facing AI tools should consider safety features, content moderation, privacy, security, age appropriateness and the needs of students with SEND.
- Apricot will keep its approach under review as technology, statutory guidance and educational practice develop.

15. Misinformation, Disinformation and Manipulated Media

Students should be supported to evaluate the reliability, source, purpose and context of online information. This includes recognising misinformation, deliberate disinformation, manipulated images, deepfakes, misleading advertising and AI-generated content.

Curriculum and teaching opportunities should encourage critical thinking, verification of sources and responsible sharing.

16. Digital Images, Video and Recordings

Images and recordings can create safeguarding, privacy and reputational risks. Apricot will use them only for legitimate educational, safeguarding, quality, operational or authorised promotional purposes.

- Staff must not use personal devices to make unauthorised recordings or photographs of students.
- Lesson recordings must remain within approved systems and access must be restricted appropriately.
- Student images or identifiable recordings must not be used publicly without an appropriate lawful basis and required permissions.
- Students must not capture or distribute images, recordings or screenshots of staff or other students without authorisation.
- Any concern about misuse of images or recordings must be reported.

17. Communications

Digital communication between staff and students or parents/carers must be professional in tone, content, timing and purpose and must use approved systems.

- Staff must not use personal email, social-media direct messages or personal messaging accounts for routine student communication.
- Messages that are threatening, sexual, abusive, discriminatory, coercive or otherwise concerning must be reported to the DSL where safeguarding is engaged.
- Users should be alert to phishing, malicious links, suspicious attachments and impersonation.
- Confidential or personal information must be shared only through appropriate secure routes.
- Where email or platform activity is monitored for security or safeguarding purposes, this will be handled in accordance with applicable privacy and data-protection requirements.

18. Passwords, Accounts and Cyber Security

- Passwords must be strong, unique and kept confidential.
- Multi-factor authentication must be used where required or provided.
- Users must lock or secure devices when unattended.
- Suspected compromise, phishing, malware or unauthorised access must be reported immediately.
- Access rights should reflect the user's role and be removed or amended promptly when no longer required.
- Software and devices under Apricot's control should be maintained and updated appropriately.
- Staff must not deliberately bypass security controls or install unauthorised software that creates organisational risk.

19. Personal Devices and Home Working

Apricot staff work remotely and may use personal devices in accordance with organisational requirements. Staff remain responsible for protecting student information and maintaining professional boundaries regardless of location.

- Work must be undertaken in a way that prevents unauthorised people from seeing or hearing confidential information where reasonably possible.
- Devices used for work must be appropriately secured.
- Student data should not be downloaded or stored locally unless there is an approved operational reason and appropriate protection.
- Family members or other third parties must not use a staff member's Apricot account.
- Printed confidential information should be avoided where possible and disposed of securely where printing is necessary.

20. Data Protection and Privacy

Personal data will be handled in accordance with Apricot's Data Protection and Privacy Policy, the Data Protection Act 2018, UK GDPR and other applicable data-protection requirements.

Online-safety monitoring, recordings and technical logs can contain personal data. Access must therefore be proportionate, purposeful and restricted to authorised people.

21. Students with SEND and Additional Vulnerabilities

Online-safety arrangements must consider individual needs. Students with SEND, communication difficulties, social isolation, anxiety or other vulnerabilities may experience online risks differently or may need additional support to recognise, report or recover from harm.

Staff should avoid assuming that a student's online behaviour is explained solely by SEND and should consider whether a change in behaviour, communication or engagement may indicate a safeguarding concern.

22. Education and Training

22.1 Students

Online-safety education will be age-appropriate, revisited regularly and embedded through relevant curriculum areas including Computing and PSHE. It will include safe communication, privacy, relationships, consent, reporting, cyberbullying, grooming, exploitation, scams, misinformation, AI, digital footprints and responsible use of technology.

22.2 Staff

Staff receive online-safety information at induction and through ongoing safeguarding and professional development. Training will reflect Apricot's remote model and emerging risks.

22.3 Parents and Carers

Apricot will provide or signpost useful online-safety information to parents/carers where appropriate, particularly where home devices, social media, AI tools or online behaviour create risks relevant to a student's education or welfare.

23. Responding to Online Safety Incidents

1. Protect immediate safety. If a child or another person is in immediate danger, contact the DSL urgently and emergency services where necessary.
2. Do not investigate a safeguarding concern independently.
3. Preserve appropriate evidence such as dates, usernames, URLs, messages or screenshots where lawful and safe, but do not download or circulate illegal child sexual abuse material.
4. Report safeguarding concerns promptly to the DSL/DDSL and record them through Apricot's safeguarding arrangements.
5. Report technical or security incidents to the appropriate IT/management contact.
6. The DSL or senior leader will assess whether the commissioner, parent/carers, platform provider, police, children's social care, LADO or another agency should be informed.
7. Take proportionate action to contain the incident, support affected individuals and reduce recurrence.
8. Record decisions, actions and outcomes.

24. Illegal Content and Criminal Activity

Where online activity may involve child sexual abuse material, grooming, threats, stalking, fraud, hate crime, extremist offences, malicious communications, serious harassment or other criminal conduct, Apricot will follow safeguarding procedures and seek police or specialist advice where appropriate. Staff must not unnecessarily view, copy, forward or store illegal content.

25. Staff Online Conduct and Allegations

Staff online conduct is subject to the same professional and safeguarding standards as conduct in any other setting. Online behaviour that breaches professional boundaries, creates a safeguarding concern or may bring suitability to work with children into question must be reported in accordance with the Staff Code of Conduct, Managing Allegations Against Staff Members Policy and low-level concerns arrangements.

A staff member must never enter into a personal online relationship with a student.

26. Monitoring, Review and Continuous Improvement

This policy will be reviewed at least annually and sooner where significant changes in technology, statutory guidance, organisational systems or safeguarding risks require it.

The review will consider, as appropriate:

- online-safety and safeguarding incidents;
- filtering and monitoring coverage, limitations and effectiveness;
- changes to Apricot's platforms and technical environment;
- student risk profiles and SEND considerations;
- staff, student, parent/carers and commissioner feedback;
- emerging risks including generative AI and synthetic media;
- cyber-security events and data incidents; and
- learning arising from complaints, allegations or quality assurance.

Appendix 1 - Online Safety Quick Guide for Staff

- Use approved Apricot systems only.
- Keep passwords and accounts secure.
- Maintain professional boundaries online.
- Do not connect with students through personal social media.
- Do not make personal recordings of students or lessons.
- Check before screen sharing.
- Treat changes in online attendance, communication or behaviour as potentially significant.
- Report concerning content, contact or conduct to the DSL.
- Never ask a child to forward an intimate image.
- Do not put confidential student information into public AI tools.
- Report suspicious links, phishing or account compromise.
- If a child is in immediate danger, act immediately - online provision does not mean waiting for the commissioner to respond.

Appendix 2 - Online Safety Risks Particularly Relevant to Apricot

- Unauthorised entry to virtual classrooms or sharing of lesson links.
- Third-party interference in a lesson from within the student's home.
- Safeguarding indicators being less visible where cameras are not used.
- Students accessing lessons through unmanaged home networks or personal devices.
- Cyberbullying or harassment affecting attendance and engagement.
- Grooming or exploitation through social media, gaming, messaging or online communities.
- Screen sharing that accidentally exposes personal or inappropriate material.
- Phishing or impersonation targeting staff or students.
- Sharing or manipulation of lesson recordings, screenshots or images.
- AI-generated sexual imagery, deepfakes or impersonation.
- Unsafe or inappropriate use of generative AI.
- Misinformation, disinformation and harmful algorithmic content.
- Online scams, financial exploitation and inappropriate commercial content.
- Over-sharing of personal details, location or private information.

Appendix 3 - Filtering and Monitoring Review Questions

- What Apricot systems and devices are currently subject to filtering or monitoring?
- What is outside Apricot's technical control, including personal devices, home broadband and commissioner-managed equipment?
- Can users be identified reliably from alerts or logs?
- Are controls effective when users work remotely?
- Are harmful, illegal, dynamic and AI-generated risks considered?
- Do controls reflect the age, SEND profile and vulnerabilities of Apricot students?
- Are staff clear about what is monitored, what is not monitored and how concerns are escalated?
- Does filtering allow legitimate curriculum access without creating unreasonable barriers?
- Are reports and alerts reviewed by appropriately trained people?
- Have incidents or near misses identified gaps that require action?
- Has the review been recorded, with actions, owners and timescales?

Authorised by: Jodie Phillips, Operations Director

Date: October 2026

Review Date: October 2027