ONLINE SAFETY POLICY

2026 – 2027

Policy Owner	**Deputy Head (Pastoral)**
Responsible Officer	Head
Approved by	Head and Governing Body
Applicable to	Whole College (Day and Boarding Students)
Last Reviewed	August 2026
Next Review	August 2027

1. Policy Statement

St Andrew's College is committed to safeguarding and promoting the welfare of all students, including their safety and wellbeing online.

The College recognises that online activity is an integral part of students' education, social lives and, for boarders, their daily lives within the College community. Online risks can arise through College-managed systems, personal devices, mobile data networks and online activity taking place away from the College.

The College will provide students with the knowledge, skills and support required to use technology safely, responsibly and positively.

Online safety is an integral part of the College's safeguarding arrangements and should not be considered solely an IT responsibility.

The College will:

- educate students about safe, responsible and respectful use of technology;
- protect students from harmful, inappropriate and illegal online content and activity;
- maintain appropriate filtering and monitoring systems;
- respond promptly to online safeguarding concerns;
- provide appropriate support following online incidents;
- ensure staff understand their online-safety responsibilities;
- promote safe and responsible use of generative artificial intelligence;

- protect personal information and maintain appropriate cyber-security arrangements; and
- work with parents, carers and boarders to promote online safety.

This policy should be read alongside the College's Safeguarding and Child Protection Policy and the related policies identified in Section 26.

2. Scope

This policy applies to:

- all students;
- all teaching, pastoral, boarding and support staff;
- the Proprietor/Governing Body;
- volunteers;
- contractors;
- homestay hosts, where applicable;
- visitors; and
- other persons using College systems or participating in College-managed activities.

It applies to:

- College-owned devices;
- personal devices connected to College networks;
- College Wi-Fi;
- College accounts and platforms;
- personal mobile data used by students;
- online learning platforms;
- social media;
- messaging services;
- gaming platforms;
- generative AI tools;

- online activity during boarding;
- online activity during educational visits and trips; and
- online activity outside College where it affects the safety, welfare or education of students or the wider College community.

For students under 18, the College's safeguarding responsibilities under Keeping Children Safe in Education apply. Students aged 18 and over remain subject to the College's online-safety, behaviour, welfare and IT expectations, although the legal framework applicable to adults differs.

3. Legal and Regulatory Framework

The College will have regard to and comply with applicable legislation, statutory guidance and regulatory requirements, including:

- Keeping Children Safe in Education 2026;
- the Education (Independent School Standards) Regulations 2014 and current DfE guidance;
- the National Minimum Standards for Boarding Schools;
- the Prevent Duty;
- the Equality Act 2010;
- the Data Protection Act 2018 and applicable UK data protection legislation;
- relevant safeguarding legislation;
- the DfE Filtering and Monitoring: Core Standard;
- the DfE digital and technology standards;
- DfE guidance on generative artificial intelligence in education;
- DfE guidance on searching, screening and confiscation;
- DfE statutory guidance on mobile phones in schools; and
- relevant cyber-security guidance.

The College will review this policy when significant changes are made to legislation, statutory guidance, regulatory requirements or recognised online-safety risks.

4. Online Safety Risks

The College recognises four broad categories of online risk:

4.1 Content

Students may encounter harmful, inappropriate or illegal material, including:

- pornography;
- violent or graphic material;
- content promoting self-harm or suicide;
- extremist or terrorist content;
- hateful or discriminatory content;
- misinformation and disinformation;
- scams and fraudulent content;
- harmful challenges;
- inappropriate sexual content; and
- AI-generated harmful material.

4.2 Contact

Students may be contacted by:

- strangers;
- adults seeking inappropriate relationships;
- individuals seeking to exploit or manipulate them;
- scammers;
- extremist groups;
- abusive peers or former partners; or
- other individuals presenting a safeguarding risk.

4.3 Conduct

Students may experience or participate in:

- cyberbullying;
- harassment;

- sexual harassment;
- sharing of intimate images;
- non-consensual image sharing;
- impersonation;
- harmful livestreaming;
- online abuse;
- discriminatory behaviour;
- manipulation;
- online coercion; and
- other harmful behaviour.

4.4 Commerce

Students may be exposed to:

- financial scams;
- phishing;
- fraud;
- gambling;
- financial exploitation;
- fraudulent online marketplaces;
- sextortion or financially motivated sexual extortion; and
- inappropriate commercial activity.

The College will educate students about these risks and respond to concerns in accordance with safeguarding and behaviour procedures.

5. Roles and Responsibilities

5.1 Proprietor/Governing Body

The Proprietor/Governing Body will:

- provide strategic oversight of online safety;

- ensure that appropriate safeguarding arrangements are in place;
- ensure appropriate filtering and monitoring systems are maintained;
- receive appropriate assurance regarding the effectiveness of online-safety arrangements;
- ensure that the policy is reviewed annually; and
- ensure that adequate resources and training are available.

The Proprietor/Governing Body will understand the relationship between online safety, filtering and monitoring, safeguarding and cyber security.

5.2 Head

The Head has overall responsibility for ensuring that the College implements this policy effectively.

5.3 Designated Safeguarding Lead

The DSL will:

- provide safeguarding oversight of online safety;
- ensure online safeguarding concerns are appropriately recorded and managed;
- liaise with IT and senior leaders regarding filtering and monitoring concerns;
- ensure emerging online risks are communicated to staff;
- ensure relevant safeguarding referrals are made;
- monitor online-safety trends and incidents; and
- contribute to staff training.

5.4 Senior Leader Responsible for Filtering and Monitoring

The designated senior leader will:

- oversee the College's filtering and monitoring arrangements;
- ensure that responsibilities are clearly assigned;
- ensure the effectiveness of filtering and monitoring is reviewed at least annually;
- work with the DSL and IT provider;
- ensure safeguarding risks inform filtering and monitoring decisions; and
- provide appropriate assurance to senior leadership and governance.

Detailed technical requirements are set out in the College's **Filtering and Monitoring Policy**.

5.5 IT Manager/Network Provider

The IT team or appointed provider will:

- maintain appropriate filtering and monitoring systems;
- maintain appropriate network and account security;
- support the safe use of digital platforms;
- maintain appropriate technical records;
- investigate technical concerns;
- report significant issues to the appropriate senior leader and DSL; and
- support the annual review of filtering and monitoring effectiveness.

5.6 Boarding Staff

Boarding staff will:

- implement the College's boarding device expectations;
- support students to use technology safely;
- respond to online-safety concerns;
- report safeguarding concerns to the DSL;
- follow arrangements concerning devices during sleeping and study periods; and
- recognise the additional online risks arising from students living together.

5.7 All Staff

All staff will:

- model safe and professional use of technology;
- maintain appropriate professional boundaries online;
- use College-approved communication systems;
- protect passwords and accounts;
- follow the Staff Code of Conduct;
- report online-safety concerns promptly;

- report inappropriate or accidental access to harmful material;
- follow searching and confiscation procedures;
- participate in online-safety and safeguarding training; and
- follow College arrangements for the use of generative AI.

5.8 Students

Students will:

- follow the Acceptable Use Agreement;
- use College systems responsibly;
- protect passwords and account information;
- respect others online;
- report concerns to a trusted adult;
- not deliberately circumvent College filtering or monitoring;
- follow boarding and mobile-device expectations;
- use generative AI responsibly and in accordance with College expectations; and
- comply with the Behaviour Policy.

6. Education and Digital Literacy

Online safety will be addressed through the College's curriculum, PSHE, tutorials, boarding provision, assemblies and wider enrichment.

Education will include, as appropriate:

- privacy and personal information;
- passwords and account security;
- digital footprints;
- online reputation;
- social media;
- healthy online relationships;
- cyberbullying;

- sexual harassment and online sexual behaviour;
- image sharing;
- scams and fraud;
- phishing;
- financial exploitation;
- online radicalisation and extremism;
- misinformation and disinformation;
- manipulated and AI-generated content;
- deepfakes;
- generative AI;
- online gaming;
- livestreaming;
- location sharing;
- online grooming and exploitation;
- reporting mechanisms; and
- maintaining healthy boundaries and wellbeing online.

Students will be encouraged to think critically about online information and to understand that content encountered online may be inaccurate, manipulated or deliberately harmful.

7. Filtering and Monitoring

The College will maintain appropriate filtering and monitoring arrangements to safeguard students.

Filtering is preventative and seeks to restrict access to illegal, inappropriate and potentially harmful content.

Monitoring is reactive and identifies activity that may indicate safeguarding or other risks.

The College will ensure that:

- filtering and monitoring responsibilities are clearly assigned;
- systems are appropriate to the College's safeguarding risks;
- systems identify users where appropriate so that concerns can be traced;
- filtering does not unreasonably restrict legitimate educational activity;
- monitoring is proportionate and appropriate;
- filtering and monitoring effectiveness is reviewed at least annually;
- safeguarding concerns identified through monitoring are referred appropriately;
- staff understand how to report concerns;
- students are informed about relevant expectations; and
- technical arrangements are reviewed when significant new risks arise.

The College's detailed arrangements are set out in the **Filtering and Monitoring Policy**.

8. Personal Mobile Data and Connectivity

The College recognises that students may use personal devices with independent mobile data connections.

Mobile data may bypass College network filtering and monitoring.

Students must therefore:

- use mobile data responsibly;
- comply with the Online Safety Policy and Acceptable Use Agreement;
- not deliberately use mobile data to access content that is prohibited under College rules;
- not use personal connectivity to deliberately circumvent College safeguarding controls; and
- comply with boarding and study-time arrangements.

The College may impose reasonable restrictions on personal connectivity where necessary to safeguard students, maintain appropriate boarding routines or prevent misuse.

Any deliberate attempt to access harmful or illegal material through personal connectivity will be dealt with under the Behaviour Policy and, where appropriate, safeguarding procedures.

9. Mobile Phones and Smart Devices

The College will implement the DfE statutory guidance on mobile phones in accordance with its status as a boarding school.

Mobile phones and other smart communication devices will not be used during the teaching day except where permitted by the College for a specific educational, medical, accessibility or safeguarding purpose.

Boarding arrangements will distinguish between the teaching day and students' residential time.

The College will establish clear arrangements for:

- storage or access during the teaching day;
- permitted use during boarding time;
- study periods;
- sleeping hours;
- contact with parents and families;
- emergency communication;
- safeguarding circumstances; and
- reasonable adjustments.

As a boarding school, the College will ensure that boarders are able to communicate privately with their parents or families at appropriate times, including consideration of different time zones for international students.

Sixth-form students may be given greater independence in relation to personal devices at specified times and locations, provided that this does not compromise safeguarding or the College's wider mobile-phone arrangements.

10. Boarding and Online Safety

The College recognises that boarding creates additional online-safety considerations because students may use personal devices within residential accommodation, often outside normal school hours.

Boarding staff will support students in managing:

- device use at night;
- online relationships;
- social media;
- gaming;
- messaging;
- livestreaming;
- location sharing;
- contact with unknown individuals;
- online exploitation;
- harmful content;
- personal mobile data; and
- online conflict between students.

Boarding staff will not routinely monitor students' private communications.

Where there is a safeguarding or serious welfare concern, appropriate action will be taken in accordance with the Safeguarding Policy and relevant College procedures.

Students will be educated about the particular risks associated with online activity within shared residential environments.

11. Acceptable Use

Students must:

- use College networks and devices responsibly;
- keep passwords and login details secure;
- not access another person's account without permission;

- not deliberately circumvent filtering or monitoring;
- not use technology to bully, harass, threaten or intimidate others;
- not create, share or distribute harmful or illegal material;
- not share intimate images of another person without consent;
- not use College systems to facilitate illegal activity;
- seek permission before photographing, filming or recording others where required;
- respect intellectual property and copyright;
- report suspicious or inappropriate activity;
- follow College rules when using personal devices; and
- follow the Acceptable Use Agreement.

Breaches will be dealt with under the Behaviour Policy and, where appropriate, the Safeguarding Policy.

12. Generative Artificial Intelligence

The College recognises that generative AI can provide educational opportunities but also creates safeguarding, privacy, ethical, academic and security risks.

Students and staff must only use AI tools in accordance with College expectations and any approved-use arrangements.

Students must not:

- provide personal, sensitive or confidential College information to unauthorised AI systems;
- use AI to generate harmful, abusive or discriminatory content;
- use AI to impersonate another person;
- create or distribute harmful deepfakes;
- generate or share sexualised images of real people;
- use AI to facilitate bullying, harassment or exploitation;
- use AI to circumvent College safeguarding or filtering controls; or

- use AI in assessed work in a way that breaches academic or examination requirements.

Students should understand that AI-generated information may be inaccurate, biased, manipulated or inappropriate.

The College will consider the age restrictions, safety features, filtering, monitoring, privacy and data-protection arrangements of AI tools before approving their use.

Any safeguarding concern arising from AI use will be referred to the DSL.

The College's approach will reflect current DfE guidance and product safety standards for generative AI.

13. Social Media and Online Communication

Students are expected to use social media responsibly and respectfully.

Students must not use social media or messaging platforms to:

- bully or harass others;
- spread discriminatory or hateful material;
- share private or confidential information;
- share intimate images without consent;
- impersonate others;
- threaten or intimidate;
- facilitate exploitation;
- deliberately damage another person's reputation; or
- bring harmful online behaviour into the College community.

Online behaviour which occurs away from College may still be addressed where it affects the safety, welfare, relationships or education of students or staff.

Staff must maintain appropriate professional boundaries and must use College-approved communication channels when communicating with students.

14. Child-on-Child Abuse and Online Sexual Harm

The College recognises that online platforms may be used to facilitate child-on-child abuse and other harmful behaviour between students.

This may include:

- sexual harassment;
- sexual violence;
- unwanted sexual communication;
- sharing or requesting intimate images;
- non-consensual image sharing;
- coercion;
- sexualised bullying;
- online grooming;
- threats;
- sextortion; and
- other harmful sexual behaviour.

Any concern involving a student under 18 will be referred to the DSL and managed in accordance with the Safeguarding and Child Protection Policy.

Where adult students are involved, concerns will be managed in accordance with safeguarding, welfare, behaviour and other relevant College procedures, taking account of the students' legal status.

Students will be taught that sharing an intimate image without consent can cause serious harm and may have legal consequences.

The College will never require students to share intimate images as part of an investigation.

15. Harmful or Illegal Content on Personal Devices

Students may arrive at College with material already stored on their personal devices.

Students will receive appropriate information during induction about:

- UK law;

- College expectations;
- online safety;
- prohibited content; and
- reporting concerns.

Where staff have a legitimate safeguarding or disciplinary concern regarding material stored on a device, the device may be searched, screened or confiscated only by authorised staff and in accordance with the College's **Searching, Screening and Confiscation Policy/Procedure**, the Behaviour Policy, safeguarding procedures and relevant guidance.

Staff must not undertake informal or unnecessary searches of students' devices.

Where potentially illegal or safeguarding-related material is identified:

- staff must not circulate, copy or unnecessarily view the material;
- the DSL must be informed immediately where appropriate;
- relevant evidence should be preserved where necessary;
- students must not be instructed to delete potentially evidential material unless this has been authorised through the appropriate safeguarding or investigative process; and
- the College will determine whether referral to the Police, children's social care or another external agency is required.

The College will respond proportionately to incidents involving young people and will take account of the nature, circumstances and safeguarding context of the material.

16. Searching and Confiscation of Electronic Devices

Searching or confiscation of an electronic device will only be undertaken in accordance with:

- the College's Searching, Screening and Confiscation Policy/Procedure;
- the Behaviour Policy;
- safeguarding procedures;
- applicable DfE guidance; and
- the legal rights and responsibilities of the College and the student.

Only staff authorised to undertake searches may do so.

A search should be proportionate to the concern and should respect the student's privacy while prioritising safeguarding.

Where a search identifies a safeguarding concern, the DSL must be informed.

17. Prevent and Online Radicalisation

The College recognises that the internet may be used to expose students to extremist material, radicalisation and harmful ideologies.

Students will receive age-appropriate education about:

- extremist content;
- manipulation and recruitment;
- misinformation;
- online echo chambers;
- critical thinking;
- reporting concerns; and
- safe and lawful online behaviour.

Concerns about radicalisation or extremist content will be referred to the DSL and managed in accordance with the College's Prevent and safeguarding arrangements.

18. Cyber Security and Account Safety

The College recognises that cyber security is part of safeguarding because cyber incidents can compromise personal information, disrupt education and create risks to student welfare.

Students and staff must:

- protect passwords;
- use multi-factor authentication where required;
- not share account credentials;
- report suspected phishing;
- not install unauthorised software where prohibited;

- report suspected account compromise;
- follow College device-security requirements; and
- protect confidential and personal information.

The College will maintain appropriate technical security arrangements in accordance with the DfE digital and technology standards.

19. Data Protection and Privacy

Online activity will be managed in accordance with applicable data-protection legislation and the College's Data Protection Policy and Privacy Notice.

The College will take appropriate steps to protect:

- personal information;
- photographs and videos;
- student records;
- safeguarding information;
- login details;
- communications; and
- other confidential information.

Filtering and monitoring arrangements will be implemented proportionately and transparently.

The College will consider data protection when selecting and using online platforms, digital services and generative AI tools.

20. Remote and Online Learning

Where remote or online learning is required, the same safeguarding and professional standards apply as during face-to-face education.

Staff will:

- use approved platforms;
- use College accounts;
- maintain professional boundaries;

- avoid unnecessary use of personal contact details;
- follow appropriate recording arrangements;
- protect student information; and
- report safeguarding concerns.

Students will:

- behave respectfully;
- follow the Acceptable Use Agreement;
- protect login details;
- use appropriate backgrounds and settings;
- not record or distribute lessons without permission; and
- report concerns.

Any safeguarding disclosure made during online learning will be managed under the Safeguarding and Child Protection Policy.

21. Staff Online Conduct

Staff must maintain professional boundaries in all online interactions with students.

Staff must:

- use College-approved communication channels;
- use College accounts where required;
- not use personal social-media accounts to communicate with students;
- not share personal contact information unnecessarily;
- maintain appropriate professional language;
- protect student information;
- follow the Staff Code of Conduct;
- follow data-protection requirements; and
- report any safeguarding concern immediately.

Accidental access to inappropriate material, inappropriate contact from a student or other online safeguarding concern must be reported to the DSL or appropriate senior leader.

22. Parents and Guardians

The College will provide parents and guardians with appropriate information and guidance to support online safety.

Parents and guardians are encouraged to:

- reinforce safe online behaviour;
- support College expectations concerning devices;
- discuss online relationships and communication with students;
- encourage students to report concerns;
- cooperate with safeguarding arrangements; and
- inform the College of significant online concerns affecting a student's welfare.

The College recognises that many students are international and may have parents or guardians living in different countries and time zones. Communication will therefore be managed sensitively and appropriately.

23. Responding to Online Safety Incidents

All staff must report online-safety concerns promptly.

Where a concern may involve safeguarding, the DSL must be informed immediately.

Examples include:

- online abuse;
- exploitation;
- grooming;
- sexual harassment or sexual violence;
- intimate-image incidents;
- sextortion;
- child-on-child abuse;

- self-harm or suicide-related content;
- radicalisation;
- extremist content;
- illegal material;
- significant cyberbullying;
- threats;
- serious scams or exploitation;
- harmful AI interactions; and
- significant breaches of online safety arrangements.

The College will:

1. establish the immediate safeguarding position;
2. refer the concern to the DSL where appropriate;
3. preserve relevant evidence where necessary;
4. support the student or students affected;
5. investigate in accordance with the appropriate procedure;
6. involve parents/guardians where appropriate;
7. refer to the Police, children's social care or other agencies where required;
8. take appropriate behaviour or disciplinary action; and
9. review whether additional preventative measures are required.

The College will not promise absolute confidentiality where information needs to be shared to safeguard a student or comply with legal obligations.

24. Recording and Information Sharing

Online-safety incidents requiring safeguarding action will be recorded securely on the College's safeguarding recording system, currently CPOMS, in accordance with the Safeguarding and Child Protection Policy.

Records will be:

- accurate;

- proportionate;
- securely stored;
- accessible to appropriate staff; and
- shared only where there is a lawful and appropriate reason to do so.

Significant incidents will be reviewed to identify wider learning or recurring patterns.

25. Monitoring, Evaluation and Governance

The College will monitor online-safety risks and the effectiveness of its arrangements.

Monitoring may include:

- filtering alerts;
- monitoring alerts;
- attempted circumvention of controls;
- online safeguarding incidents;
- cyberbullying;
- sexual-image incidents;
- AI-related incidents;
- radicalisation concerns;
- device misuse;
- boarding-related online incidents;
- mobile-data misuse; and
- student and staff feedback.

The DSL and designated senior leader will review relevant information and identify emerging risks.

Significant trends and concerns will be reported through appropriate safeguarding and governance arrangements.

The effectiveness of filtering and monitoring will be reviewed at least annually and following significant changes in technology, safeguarding risk or College provision.

26. Training

All staff will receive appropriate online-safety and safeguarding training as part of the College's safeguarding training programme.

Training will include, as appropriate:

- online safeguarding risks;
- filtering and monitoring;
- reporting procedures;
- cyber security;
- online sexual harm;
- child-on-child abuse;
- online radicalisation;
- social media;
- generative AI;
- data protection;
- device searching;
- emerging online risks; and
- boarding-specific online-safety considerations.

Staff will be updated when significant new risks or guidance emerge.

Students will receive regular online-safety education appropriate to their age, maturity, circumstances and level of independence.

27. Related Policies and Procedures

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Filtering and Monitoring Policy;
- Behaviour Policy;
- Suspensions and Permanent Exclusions Procedure;
- Anti-Bullying Policy;

- Searching, Screening and Confiscation Policy/Procedure;
- Prevent Policy/Prevent arrangements;
- Acceptable Use Agreement;
- Staff Code of Conduct;
- Data Protection Policy;
- Privacy Notice;
- SEND Policy;
- Boarding Handbook and Boarding Policies;
- Mobile Phone/Personal Device arrangements;
- Remote Learning arrangements; and
- Complaints Policy.

Where there is a conflict between this policy and the Safeguarding and Child Protection Policy, safeguarding requirements will take precedence.

28. Review

This policy will be reviewed annually, or sooner where required by:

- changes in legislation;
- changes to Keeping Children Safe in Education;
- changes to the Independent School Standards;
- changes to the National Minimum Standards for Boarding Schools;
- changes to DfE filtering and monitoring standards;
- changes in technology;
- emerging online-safety risks;
- significant incidents; or
- findings from monitoring, governance or inspection.

The next scheduled review is **August 2027**.