APEX2100

ONLINE SAFETY AND ACCEPTABLE USE POLICY

Academic Year: 2026–2027
Policy Owner: Apex2100 Education Board
Designated Safeguarding Lead (DSL): Dave Breen
Deputy Designated Safeguarding Leads (DDSLs): Karen Thomas, Stuart Terris and Mark Tilston
Designated Safeguarding Governor / Board Lead: Mike Buchanan
Review frequency: At least annually and sooner where legislation, statutory guidance or Academy practice changes
Presented to Board: September 2026
Next scheduled review: September 2027

---

1. Policy Statement

Apex 2100 recognises that technology is an important part of education, communication, training and everyday life.
The Academy is committed to ensuring that students can use technology safely, responsibly and positively.
Online safety is an integral part of safeguarding.
The Academy recognises that students may experience online risks including:

- cyberbullying;
- grooming;
- sexual exploitation;
- sexual harassment;
- sexual violence;
- sharing of sexual images;
- exposure to inappropriate or illegal content;
- online scams and fraud;
- identity theft;
- hacking and cybercrime;
- extremist or terrorist content;
- radicalisation;
- criminal exploitation;
- online gambling;
- harmful online communities;
- misinformation and disinformation;
- abuse through gaming;
- livestreaming risks;
- inappropriate contact with adults;
- manipulation and coercion;
- excessive or harmful use of technology; and

- risks associated with artificial intelligence.

Apex2100 will promote a culture in which students understand online risks, make responsible decisions and know how to obtain help.

---

2. Scope
This policy applies to:

- all Apex 2100 students;
- all staff;
- governors and Board members;
- volunteers;
- contractors;
- visitors using Academy technology; and
- anyone using Academy systems, devices, networks or accounts.

It applies to:

- Academy-owned devices;
- personal devices used for Academy activities;
- Academy networks;
- Academy email accounts;
- educational platforms;
- messaging systems;
- social media;
- gaming platforms;
- cloud services;
- artificial intelligence tools; and
- other digital services used in connection with Apex2100.

The policy applies whether technology is used on or away from Academy premises where the activity affects Academy life, student welfare, Academy systems or the reputation and safety of the Academy community.

---

2. Online Safety and Safeguarding

Online activity can form part of a wider safeguarding concern.
Staff must report concerns to the DSL or DDSL where online behaviour involves:

- grooming;
- sexual exploitation;
- sexual harassment;
- sexual violence;
- sharing sexual images involving children;
- threats;
- blackmail;
- coercion;

- exploitation;
- criminal activity;
- extremist or terrorist material;
- radicalisation;
- serious bullying;
- self-harm;
- suicide-related content;
- abuse by an adult;
- trafficking; or
- any other indication that a child may be suffering or likely to suffer harm.

Online safety concerns must not be treated solely as IT problems where there is a safeguarding dimension.

---

3. Responsibilities of the Academy

Apex2100 will:

- provide age-appropriate online safety education;
- maintain appropriate filtering and monitoring;
- maintain appropriate technical security;
- provide staff training;
- establish clear acceptable-use expectations;
- respond to online safety incidents;
- support students who experience online harm;
- investigate misuse of Academy systems;
- work with parents and carers where appropriate;
- maintain appropriate records;
- review emerging technology risks; and
- regularly review online safety arrangements.

The Academy will seek to balance online safety with students' legitimate educational use of technology.

---

4. Filtering and Monitoring

The Academy will maintain appropriate filtering and monitoring systems designed to reduce exposure to harmful or inappropriate online content.
Apex2100 currently uses appropriate filtering and monitoring arrangements, including iBOSS where applicable, together with other technical controls recommended by its safeguarding and technology partners.
Filtering and monitoring will be reviewed regularly.
The Academy recognises that filtering and monitoring cannot eliminate every online risk. Students must therefore receive education enabling them to make safe decisions even where technical controls do not prevent access to harmful content.
Where monitoring identifies a potential safeguarding concern, the matter may be referred to the DSL or DDSL.

---

5. Student Acceptable Use

Students are expected to use technology responsibly.
Students must:

- use technology for legitimate educational, training or approved personal purposes;
- protect their passwords;
- keep personal information secure;
- respect the privacy of others;
- communicate respectfully;
- follow staff instructions;
- report harmful or inappropriate content;
- report suspicious online contact;
- use Academy systems appropriately;
- respect copyright and intellectual property;
- follow applicable laws; and
- take responsibility for their digital behaviour.

---

6. Students Must Not

Students must not:

- access material that they know or reasonably believe is illegal;
- deliberately bypass Academy filtering or security controls;
- attempt to access another person's account;
- share passwords;
- impersonate another person;
- distribute malicious software;
- attempt to damage Academy systems;
- use Academy systems for criminal activity;
- bully or harass others;
- send threatening messages;
- distribute humiliating material;
- share private information without permission;
- record people without appropriate consent where consent is required;
- distribute images or recordings of others inappropriately;
- share sexual images involving children;
- use technology to facilitate exploitation;
- deliberately access extremist or terrorist material;
- use Academy systems to promote hatred or discrimination; or
- engage in activity that places themselves or another person at risk.

---

7. Passwords and Account Security

Students and staff must:

- keep passwords confidential;
- use strong passwords;
- avoid using easily guessed passwords;
- not share accounts;
- log out of systems when appropriate;
- report suspected compromised accounts;
- use multi-factor authentication where provided; and
- follow Academy IT security instructions.

Staff must never ask students to provide passwords unless there is a specific authorised technical or safeguarding reason and the process complies with Academy procedures.

8. Personal Devices

Personal devices may be used where permitted by Apex2100.
Students remain responsible for ensuring that their personal devices are used appropriately.
The Academy may impose reasonable restrictions on:

- mobile phones;
- tablets;
- laptops;
- smartwatches;
- cameras;
- gaming devices;
- recording equipment; and
- other connected devices.

Where personal-device use creates a safeguarding, behavioural or educational concern, the Academy may take appropriate action.

9. Mobile Phones and Cameras

Students must use mobile phones and cameras responsibly.
Students must not:

- photograph or record another person without appropriate permission where permission is required;
- record private conversations;
- secretly record staff;
- record incidents for the purpose of humiliation or distribution;
- share images intended to embarrass or harm another person;
- photograph or record in private areas such as bathrooms or changing facilities;
- use cameras to facilitate bullying or harassment; or
- distribute inappropriate or sexualised images.

The Academy may restrict phone or camera use in particular activities or locations.

10. Images and Videos of Students

Students must respect the privacy and dignity of others.
Images or videos involving students must not be shared publicly where doing so would:

- cause harm;
- humiliate;
- threaten;
- exploit;
- harass;
- breach privacy; or
- create a safeguarding concern.

Particular care must be taken with images involving children.
The sharing of sexual images involving children must be reported immediately to the DSL or DDSL.
Students must never be encouraged to forward or redistribute such material.

---

11. Cyberbullying

Cyberbullying is prohibited.
It may include:

- abusive messages;
- threatening messages;
- online exclusion;
- rumours;
- humiliating images;
- fake accounts;
- impersonation;
- harassment;
- coordinated attacks;
- unwanted tagging;
- publication of private information;
- malicious editing of images;
- abuse through gaming platforms; or
- livestreaming abuse.

Concerns will be addressed under the Anti-Bullying and Cyberbullying Policy and, where appropriate, the Safeguarding and Child Protection Policy.

---

12. Online Sexual Harassment and Sexual Violence

Online sexual harassment and sexual violence are unacceptable.
This may include:

- sexualised messages;
- unwanted sexual comments;
- sexual threats;

- sending unwanted sexual material;
- pressure to send images;
- sharing sexual images;
- sexualised group chats;
- online sexual humiliation;
- sexual blackmail;
- threats to publish images; or
- other unwanted sexual behaviour.

Any safeguarding concern must be reported immediately to the DSL or DDSL.

---

13. Sharing Sexual Images

Students must never be pressured into creating or sharing sexual images.
Where sexual images involving children are reported:

- staff must remain calm;
- staff must not ask students to forward images;
- staff must not download or distribute illegal images;
- staff must not investigate the matter themselves;
- the concern must be reported to the DSL/DDSL immediately; and
- the Academy will determine the appropriate safeguarding response.

The Academy will consider the circumstances of all students involved and will not automatically treat the child who created or shared an image as a perpetrator.

---

14. Grooming and Online Contact With Adults

Students should be aware that people online may not always be who they claim to be.
Students should report:

- requests to keep conversations secret;
- requests for personal information;
- requests for photographs;
- sexualised conversations;
- offers of money or gifts;
- invitations to meet;
- attempts to move conversations to private platforms;
- threats or blackmail;
- manipulation;
- pressure to break rules; or
- anything that makes them feel uncomfortable or unsafe.

Students will be encouraged to seek help without fear of punishment for reporting a concern.

---

15. Social Media

Students must use social media responsibly.

They must not use social media to:

- bully;
- harass;
- threaten;
- discriminate;
- impersonate others;
- spread malicious rumours;
- share private information;
- publish inappropriate recordings;
- share sexual images;
- encourage violence;
- promote criminal activity;
- promote extremist or terrorist material; or
- deliberately damage another person's reputation.

Students should consider the long-term consequences of online activity.
Content posted online may be copied, shared or retained even after deletion.

---

16. Gaming and Online Communities

Apex2100 recognises that online gaming can provide positive social and educational opportunities but can also expose students to risks.
Students should:

- use privacy settings appropriately;
- avoid sharing personal information;
- report abusive behaviour;
- use age-appropriate services;
- avoid meeting online contacts in person without appropriate safeguards;
- report requests for private or sexual communication; and
- report financial or criminal exploitation.

The Academy will respond to gaming-related safeguarding concerns where they affect student welfare.

---

17. Livestreaming

Students must understand that livestreaming can create additional risks.
Students should not:

- livestream from private areas;
- reveal personal information;
- livestream another person without appropriate permission;
- engage in sexualised livestreaming;
- accept inappropriate requests from viewers;
- allow unknown people to control or manipulate their activity; or
- use livestreaming to bully or humiliate others.

Concerns about livestreaming must be reported to staff.

18. Artificial Intelligence

Apex2100 recognises that artificial intelligence is increasingly used in education and everyday life.
AI tools may provide educational benefits but also create risks.
Students must use AI responsibly.
They must not use AI to:

- create or distribute sexualised images of children;
- create humiliating or abusive images of another person;
- impersonate another person maliciously;
- generate threats;
- facilitate bullying;
- create fraudulent documents;
- commit cybercrime;
- evade safeguarding or security controls;
- produce discriminatory or hateful material; or
- otherwise cause harm.

Students should not enter sensitive personal information about themselves or others into AI systems unless specifically authorised.
Where AI is used for educational work, students must follow Academy expectations concerning academic integrity and attribution.

19. Deepfakes and Manipulated Media

The Academy recognises that AI can be used to create realistic but false images, audio and video.
Students must not create or distribute manipulated material intended to:

- humiliate;
- threaten;
- sexually exploit;
- harass;
- deceive;
- bully; or
- damage another person's reputation.

Sexualised deepfake images involving children will be treated as a serious safeguarding concern.
Any such concern must be reported immediately to the DSL or DDSL.

20. Online Extremism and Radicalisation

Students may encounter extremist or terrorist content online.
The Academy will provide education designed to promote:

- critical thinking;
- media literacy;
- resilience;
- respectful debate;
- understanding of misinformation;
- awareness of manipulation; and
- safe reporting of concerning material.

Concerns about radicalisation or extremist influence must be reported under the Academy's safeguarding and Prevent procedures.

---

21. Online Scams and Financial Exploitation

Students should be aware of online financial risks.
These may include:

- scams;
- phishing;
- fraudulent websites;
- fake competitions;
- requests for money;
- cryptocurrency scams;
- account theft;
- identity theft;
- blackmail; and
- criminal exploitation.

Students should report suspicious activity to a trusted adult.

---

22. Cybersecurity

Students and staff must not attempt to compromise Academy IT systems.
Prohibited activity includes:

- hacking;
- password attacks;
- unauthorised access;
- malware;
- denial-of-service attacks;
- unauthorised scanning;
- bypassing security controls;
- installing unauthorised software;
- deliberate disruption of systems; or
- accessing data without permission.

Security concerns must be reported to the appropriate Academy IT contact.
Where a cybersecurity incident has a safeguarding dimension, the DSL must also be informed.

23. Staff Acceptable Use

Staff must:

- use Academy-approved systems where available;
- maintain professional boundaries;
- communicate with students through approved channels;
- protect confidential information;
- maintain secure passwords;
- use appropriate privacy settings;
- report suspicious activity;
- follow data protection requirements;
- maintain appropriate professional social media boundaries; and
- follow the Staff Code of Conduct.

Staff must not:

- communicate privately with students through inappropriate channels;
- use personal accounts for inappropriate student communication;
- share personal or confidential student information;
- send inappropriate material;
- engage in inappropriate online relationships with students;
- connect with students through personal social media where this breaches professional boundaries; or
- use technology in a way that could undermine safeguarding.

24. Professional Boundaries Online

Online communication must maintain the same professional standards expected in face-to-face interactions.
Staff should consider:

- whether the communication is necessary;
- whether the communication is appropriate;
- whether the communication should be visible to another member of staff;
- whether the communication should be through an Academy-approved system;
- whether a record should be retained; and
- whether the communication could reasonably be misunderstood.

Concerns about staff online behaviour should be reported under the Safeguarding and Staff Code of Conduct procedures.

25. Monitoring and Privacy

The Academy recognises that students and staff have legitimate expectations of privacy. However, Academy systems may be monitored where necessary for:

- safeguarding;
- security;
- prevention of cybercrime;
- compliance;
- investigation of misuse;
- protection of Academy systems; and
- other legitimate purposes.

Monitoring will be carried out in accordance with applicable law and Academy procedures. Students should understand that activity conducted through Academy systems should not be assumed to be completely private.

26. Reporting Online Safety Concerns

Students should report concerns as soon as possible.
Concerns may be reported to:

- a member of staff;
- a trusted adult;
- the DSL;
- a DDSL;
- Academy leadership; or
- the appropriate IT support contact.

Students should not feel that they will be punished simply because they have encountered something inappropriate online.
Where a student has made a mistake online, the Academy will consider the circumstances and prioritise safeguarding and education.

27. Responding to Online Incidents

The Academy will assess each incident individually.
The response may include:

- safeguarding intervention;
- pastoral support;
- education;
- removal of harmful content where possible;
- changes to account permissions;
- technical intervention;
- parental involvement;
- behaviour intervention;
- disciplinary action;
- police involvement;
- referral to children's social care; or
- referral to other appropriate agencies.

The Academy will consider the welfare of all students involved.

28. Evidence and Preservation

Where appropriate, students may be advised to preserve evidence such as:

- screenshots;
- usernames;
- dates and times;
- messages;
- links;
- account names; and
- other relevant information.

Students must not redistribute illegal or harmful material simply to preserve evidence.
Staff will seek advice from the DSL and/or appropriate technical or safeguarding professionals where necessary.

29. Online Safety Education

Online safety education will be embedded throughout the Academy's curriculum and pastoral provision.
Students will learn about:

- privacy;
- passwords;
- online identity;
- digital footprints;
- healthy online relationships;
- consent;
- cyberbullying;
- grooming;
- exploitation;
- sexual harassment;
- sexual violence;
- image sharing;
- misinformation;
- extremist content;
- scams;
- cybersecurity;
- AI;
- deepfakes;
- responsible social media use; and
- reporting concerns.

Education will be age-appropriate and responsive to emerging risks.

30. Vulnerable Students

Some students may be at increased risk of online harm.
This may include students who:

- have SEND;
- experience social isolation;
- are vulnerable to exploitation;
- have experienced bullying;
- have safeguarding concerns;
- have difficulty communicating concerns; or
- are particularly susceptible to manipulation.

The Academy will consider additional support and reasonable adjustments where appropriate.

31. Parents and Carers

The Academy will seek to work with parents and carers to promote online safety.
Where appropriate, the Academy may provide information concerning:

- parental controls;
- social media;
- gaming;
- online exploitation;
- cyberbullying;
- age restrictions;
- AI;
- online sexual risks;
- digital wellbeing; and
- reporting harmful content.

Where a safeguarding concern exists, information may be shared in accordance with the Safeguarding and Child Protection Policy.

32. Breaches of This Policy

A breach of this policy may result in:

- education or advice;
- removal or restriction of access to technology;
- pastoral intervention;
- parental involvement;
- behavioural consequences;
- disciplinary action;
- safeguarding intervention;
- referral to the police; or
- referral to another appropriate agency.

The response will be proportionate to the circumstances.

Serious misuse of technology may constitute a safeguarding matter or criminal offence.

---

34. No Retaliation

Students must not retaliate against anyone who reports an online safety concern.
Retaliation may include:

- threats;
- further bullying;
- online abuse;
- exclusion;
- intimidation;
- publication of personal information; or
- attempts to identify or punish a person who made a report.

Retaliation will be treated seriously.

---

35. Record Keeping

Significant online safety incidents will be recorded appropriately.
Records may include:

- the nature of the concern;
- students involved;
- date and time;
- actions taken;
- safeguarding decisions;
- technical action;
- parental communication;
- referrals;
- outcomes; and
- follow-up arrangements.

Safeguarding records will be maintained in accordance with the Safeguarding and Child Protection Policy.

---

36. Links With Other Policies

This policy should be read alongside:

- Safeguarding Children and Child Protection Policy;
- Anti-Bullying and Cyberbullying Policy;
- Staff Code of Conduct;
- Behaviour and Student Conduct Policy;
- Equality, Diversity and Inclusion Policy;
- Complaints Policy; and
- Whistleblowing Policy.

---

38. Policy Review

This policy will be reviewed at least annually.

The review will consider:

- online safety incidents;
- cyberbullying;
- safeguarding concerns;
- filtering and monitoring;
- student feedback;
- staff feedback;
- technological developments;
- AI developments;
- cybersecurity incidents;
- emerging online threats;
- training;
- legislative changes; and
- lessons learned.

The policy will be reviewed sooner where a significant change in technology, law, safeguarding risk or Academy practice occurs.

APPENDIX 1
STUDENT ONLINE SAFETY – QUICK GUIDE
Think before you post
Ask yourself:

- Would I be happy for this to be seen by my family?
- Could this hurt someone?
- Could this affect my future?
- Am I sharing someone else's information?
- Am I breaking the law or Academy rules?

If something online worries you:
Stop → Don't respond → Save evidence if safe → Tell someone → Get help
You will not be in trouble simply for telling an adult that something has gone wrong online.

APPENDIX 2
STAFF QUICK GUIDE
If a student reports an online concern:

1. Listen.
2. Take the concern seriously.
3. Establish whether there is an immediate safeguarding risk.
4. Do not ask the student to forward illegal sexual images.
5. Do not investigate beyond your role.
6. Record relevant facts.
7. Report safeguarding concerns immediately to the DSL/DDSL.
8. Follow the Academy's safeguarding procedures.
9. Preserve relevant information appropriately.
10. Ensure the student receives appropriate support.

Remember
Online safety is safeguarding.
Do not assume that online behaviour stays online.
Do not promise confidentiality.
Do not forward illegal images of children.
Report safeguarding concerns without delay.