Online Safety Policy

Effective from: August 2025
Last reviewed: August 2026
Next review due: August 2027

KING'S COLLEGE SCHOOL
PANAMA

An inspired School

Purpose and Ethos

King's College School Panama is committed to safeguarding pupils and promoting their wellbeing in all aspects of School life, including the digital environment.

Online safety is an integral part of the School's safeguarding culture and wider duty of care. Technology, digital platforms and artificial intelligence are now central to learning, communication and social interaction. The School therefore aims to ensure that pupils use technology safely, responsibly, ethically and confidently while being protected from harm, exploitation, inappropriate content and emerging online risks.

Effective online safety is achieved through:

- high-quality education;
- clear behavioural expectations;
- appropriate supervision;
- robust technical systems;
- strong professional boundaries;
- effective filtering and monitoring;
- responsive safeguarding procedures; and
- a culture in which pupils feel confident to report concerns.

The School recognises that no technical system can eliminate risk completely. Education, professional judgement, safeguarding vigilance and trusted relationships remain essential.

Scope

This policy applies to:

- all pupils;
- all teaching and support staff;
- supply staff and trainee teachers;
- volunteers and contractors where relevant;
- visitors using School digital systems where appropriate; and
- parents and guardians where their use of School systems, School communication channels or online activity has a material impact on pupil safety or School life.

It applies to:

- School-owned devices and systems;
- personal devices used on School premises;
- School-managed accounts;
- online learning platforms;
- digital communication tools;
- artificial intelligence tools;
- third-party applications and services;

- remote or blended learning;
- School-related online activity outside School hours; and
- online behaviour outside School where it affects the safety, welfare, relationships or education of pupils or has a material connection with School life.

Regulatory and Guidance Framework

King's College School Panama operates within the legal and regulatory framework of Panama.

This policy is informed by:

- applicable Panamanian legislation relating to the protection, welfare and rights of children;
- relevant MEDUCA requirements;
- the Standards for British Schools Overseas;
- Keeping Children Safe in Education 2026, adopted by the School as its principal British safeguarding benchmark where compatible with Panamanian law and the international context;
- current UK Council for Internet Safety guidance;
- relevant Department for Education digital and technology standards, including filtering and monitoring expectations;
- relevant Inspired Education safeguarding and technology requirements; and
- recognised international best practice in online safety.

UK guidance may inform the School's approach as recognised British best practice but does not create statutory powers or duties for King's College School Panama under English law.

Where there is any conflict between overseas guidance and applicable Panamanian law, Panamanian law takes precedence.

Related Policies

This policy should be read alongside:

- Safeguarding and Child Protection Policy;
- Whole School Behaviour Policy;
- Preventing and Tackling Bullying Policy;
- Acceptable Use of Technology Policy;
- Mobile Phones and Electronic Equipment Policy;
- Sharing Nudes and Semi-Nudes Policy;
- Staff Code of Conduct;
- Data Protection Policy;
- PSHE Policy;
- Relationships Education, Relationships and Sex Education and Health Education Policy; and
- relevant searching, confiscation and device-management procedures.

Online Risk Categories

The School recognises that online risks are broad and often overlap.
They include:

Content

Risks arising from exposure to harmful or inappropriate material, including:

- pornography;
- violent or extremist content;
- self-harm or suicide content;
- eating-disorder content;
- hate material;
- discriminatory content;
- harmful health misinformation;
- misinformation and disinformation;
- conspiracy theories;
- harmful AI-generated content; and
- content designed to manipulate, exploit or distress.

Contact

Risks arising from interaction with others, including:

- grooming;
- sexual exploitation;
- criminal exploitation;
- coercion;
- harassment;
- stalking;
- unwanted contact;
- impersonation;
- contact from unknown adults or peers; and
- pressure to share personal information or images.

Conduct

Risks arising from a pupil's own behaviour or the behaviour of others, including:

- cyberbullying;
- child-on-child abuse;
- abusive messaging;
- discriminatory behaviour;
- online sexual harassment;
- image-based abuse;
- sharing nudes or semi-nudes;

- deepfakes or deep nudes;
- trolling;
- doxxing;
- impersonation; and
- misuse of School systems.

Commerce

Risks arising from commercial activity, including:

- scams;
- phishing;
- financial exploitation;
- gambling-related content;
- in-app purchasing;
- deceptive advertising;
- fraudulent marketplaces; and
- pressure to provide payment or banking information.

Roles and Responsibilities

Online safety is a shared responsibility.

Head of School

The Head of School has overall responsibility for ensuring that effective online-safety arrangements are in place and that online safety is integrated into the School's safeguarding strategy.

The Head ensures that:

- appropriate policies and systems are in place;
- sufficient resources and training are provided;
- responsibilities are clearly allocated;
- significant online-safety risks are reviewed;
- filtering and monitoring arrangements receive appropriate senior oversight; and
- safeguarding considerations inform decisions about technology and digital systems.

Designated Safeguarding Lead

The Designated Safeguarding Lead is Zoe Pett.

The DSL has lead safeguarding responsibility for online safety and works closely with IT and senior leaders.

The DSL:

- provides safeguarding oversight of online risks;
- ensures online safeguarding concerns are acted upon promptly;

- advises on risk and escalation;
- ensures appropriate referrals are made where necessary;
- understands the filtering and monitoring systems in place;
- reviews safeguarding trends arising from online incidents;
- supports staff dealing with online harm; and
- ensures alignment with the Safeguarding and Child Protection Policy.

Routine technical, behavioural or pastoral issues will normally be managed through IT, Heads of Phase or other appropriate School systems. The DSL will take the lead where an online concern raises a safeguarding issue or may constitute child-on-child abuse.

IT and Digital Systems Leadership

The School's IT function is responsible for the effective operation of technical safeguards.

This includes:

- filtering and monitoring;
- access controls;
- account security;
- device management;
- system logging;
- incident escalation;
- cybersecurity protections;
- software and platform controls;
- maintaining appropriate technical records; and
- supporting safeguarding and leadership teams with relevant information.

IT staff must understand that technical monitoring can reveal safeguarding information and must escalate concerns promptly to the DSL where appropriate.

Senior Leadership Team

The Senior Leadership Team:

- ensures this policy is implemented consistently;
- reviews online-safety trends;
- ensures staff receive appropriate training;
- supports appropriate curriculum provision;
- reviews significant incidents;
- ensures appropriate oversight of third-party digital tools; and
- supports the DSL and IT team in maintaining effective systems.

Heads of Phase

Heads of Phase provide operational pastoral oversight of online-safety concerns within their areas.

They:

- respond to routine online behaviour and pastoral concerns;
- support pupils affected by online incidents;
- liaise with parents and guardians where appropriate;
- identify recurring patterns or peer-group concerns;
- ensure appropriate behavioural or pastoral interventions are implemented;
- escalate safeguarding concerns promptly to the DSL; and
- work with the DSL, IT team and senior leaders where concerns cross pastoral, technical and safeguarding boundaries.

Staff

All staff are responsible for:

- modelling safe, responsible and professional online behaviour;
- maintaining appropriate professional boundaries online;
- using only approved communication channels with pupils;
- supervising pupil technology use where appropriate;
- following the Acceptable Use of Technology Policy and Staff Code of Conduct;
- remaining vigilant to signs of online harm;
- reporting safeguarding concerns without delay;
- recording safeguarding concerns appropriately on iSAMS Wellbeing Manager;
- completing required online-safety training; and
- not bypassing or undermining School filtering, monitoring or security controls.

Pupils

Pupils are expected to:

- use technology responsibly;
- follow the Acceptable Use of Technology Policy;
- treat others with respect online;
- protect personal information;
- use School accounts and systems appropriately;
- not attempt to bypass filtering or security controls;
- report anything online that makes them feel unsafe, uncomfortable or concerned;
- not create, share or amplify harmful content;
- use artificial intelligence tools responsibly and in accordance with School expectations; and
- seek help from a trusted adult when needed.

Parents and Guardians

Parents and guardians are encouraged to:

- support safe and responsible online behaviour at home;
- maintain appropriate oversight of their child's digital use;
- engage with School guidance on online safety;

- report concerns promptly;
- avoid escalating pupil disputes through social media or group chats;
- reinforce age-appropriate boundaries around devices and platforms; and
- work constructively with the School where online concerns arise.

Education and Prevention

The School adopts a proactive and preventative approach to online-safety education.

Pupils are taught in an age-appropriate and progressive way through:

- PSHE;
- computing;
- Relationships Education and RSE;
- assemblies;
- tutor and pastoral programmes;
- curriculum subjects;
- targeted interventions; and
- responsive sessions addressing emerging risks.

Education includes:

- digital citizenship;
- privacy and personal information;
- passwords and account security;
- cyberbullying;
- child-on-child abuse;
- online relationships;
- grooming and exploitation;
- harmful content;
- misinformation and disinformation;
- manipulated media;
- generative AI;
- deepfakes and synthetic media;
- image sharing;
- online sexual harm;
- social media;
- scams and financial exploitation;
- reporting concerns; and
- how to access help.
-

Teaching will be adapted where necessary for pupils with SEND or other vulnerabilities.

Generative AI and Synthetic Media

The School recognises that generative AI creates significant educational opportunities alongside new safeguarding and behavioural risks.

These may include:

- creation of false or harmful content;
- impersonation;
- deepfakes;
- deep nudes;
- sexualised AI-generated imagery;
- harassment;
- fabrication of evidence;
- misinformation;
- manipulation;
- inappropriate automated advice; and
- exposure to harmful or age-inappropriate outputs.
- Pupils must not use generative AI to:
- create harmful, humiliating, abusive or deceptive content;
- impersonate another person;
- create or distribute sexualised imagery of another person;
- fabricate evidence;
- threaten, coerce or harass;
- bypass School safeguards; or
- engage in behaviour prohibited by School policies.

Any AI-generated sexual imagery involving a child will be treated as a safeguarding matter.

Pupils and staff must not enter personal, sensitive, confidential or safeguarding information into generative AI tools unless the tool has been specifically approved for that purpose and its use complies with the School's data-protection requirements.

The School will review the suitability of AI tools before approving them for use and will consider:

- age appropriateness;
- data protection;
- privacy;
- moderation;
- product safeguards;
- filtering;
- monitoring;
- risk of harmful outputs; and
- educational value.

Online Sexual Harm and Image Sharing

The School treats online sexual harm as a serious safeguarding matter.

This may include:

- sexual harassment;
- pressure to share images;
- sharing nudes or semi-nudes;
- non-consensual distribution of images;
- sexualised bullying;
- coercion;
- sextortion;
- image manipulation;
- deep nudes;
- sexualised deepfakes; and
- other forms of image-based abuse.

All incidents involving nude or semi-nude imagery involving a person under 18 require a safeguarding response. Staff must not routinely:

- view;
- download;
- copy;
- print;
- save;
- forward; or
- share such images.

The procedures in the Sharing Nudes and Semi-Nudes Policy must be followed.

Filtering and Monitoring

The School maintains appropriate filtering and monitoring systems to reduce the risk of pupils accessing harmful content or engaging in unsafe online behaviour.

The systems in place should be appropriate to:

- the age range of pupils;
- the curriculum;
- the School's device environment;
- School-owned and managed accounts;
- use of cloud-based services;
- online learning platforms;
- emerging technologies;

- generative AI; and
- the School's current safeguarding risk profile.

Filtering should seek to restrict access to harmful and inappropriate content without unreasonably restricting legitimate teaching and learning.

Monitoring should support the identification of:

- safeguarding concerns;
- harmful searches or activity;
- attempts to access prohibited material;
- indicators of exploitation;
- cyberbullying;
- sexualised harm;
- extremist or violent content;
- self-harm or suicide-related searches;
- misuse of School systems; and
- other concerning patterns.

No filtering or monitoring system replaces professional vigilance, supervision or education.

When reviewing filtering and monitoring arrangements, the School will consider the age and developmental stage of pupils, frequency and nature of technology use, pupils who may be at greater risk of harm, and the proportionality of technical controls to identified safeguarding risks.

Filtering and monitoring arrangements will be proportionate to the identified safeguarding risk and implemented in accordance with applicable privacy and data-protection requirements. Pupils and staff will be informed, in an age-appropriate and transparent manner, that School systems and devices may be subject to filtering and monitoring.

Governance of Filtering and Monitoring

The School will:

- identify named individuals with responsibility for filtering and monitoring;
- ensure the DSL understands the systems in place;
- ensure IT staff understand safeguarding escalation requirements;
- review filtering and monitoring arrangements at least annually;
- review arrangements sooner where technology, risk or systems change materially;
- verify, as part of the annual review, that filtering is operating appropriately across all relevant School-managed internet-connected devices and locations;
- test whether filtering and monitoring arrangements are functioning as intended;
- consider the impact of generative AI, personalised and dynamic content;
- ensure reasonable access for legitimate educational use;

- ensure staff know how to report concerns about filtering or monitoring effectiveness; and
- retain a record of the review, checks undertaken, findings and any resulting actions.

Significant weaknesses will be escalated promptly to the Head of School and appropriate Inspired Education leadership.

Personal Devices and BYOD

Use of personal devices must comply with the Mobile Phones and Electronic Equipment Policy and Acceptable Use of Technology Policy.

Where personal devices are permitted:

- pupils must follow School rules;
- School systems and networks must not be deliberately bypassed;
- inappropriate content must not be accessed, created or shared;
- privacy of others must be respected;
- devices must not be used to photograph, record or distribute content without appropriate permission; and
- the School may restrict or withdraw access where necessary.

Personal-device use does not reduce the School's expectation that pupils behave safely and responsibly.

Staff Professional Boundaries and Communication

Staff must maintain professional boundaries in all digital communication with pupils.
Staff must:

- use only School-approved accounts and communication platforms;
- not communicate with pupils through personal social-media accounts;
- not use personal messaging services with pupils unless specifically authorised under an approved School process;
- maintain appropriate tone, timing and content;
- preserve records where necessary;
- avoid private or secret communications;
- comply with the Staff Code of Conduct; and
- report any communication that may create a safeguarding concern.

Third-Party Platforms and Digital Tools

Digital platforms, applications and AI tools used with pupils must be appropriately approved by the School before use.

Approval will take account of:

- educational purpose;

- age suitability;
- safeguarding risk;
- privacy;
- data protection;
- security;
- moderation;
- advertising;
- data collection;
- AI functionality;
- user-generated content;
- safeguarding features; and
- applicable terms of service.

Use of a third-party platform does not transfer the School's safeguarding responsibilities.

Cybersecurity and Account Safety

The School expects all users to protect accounts and systems.

Users must:

- keep passwords secure;
- not share login details;
- use multi-factor authentication where required;
- report suspected account compromise;
- avoid phishing and suspicious links;
- not install unauthorised software;
- not attempt to access restricted systems; and
- follow School cybersecurity instructions.

Suspected breaches will be reported promptly to IT and, where relevant, the DSL or Data Protection lead.

Reporting Online-Safety Concerns

Pupils may report an online-safety concern to any trusted adult.

Parents may report concerns to:

- the pupil's Class Teacher or Form Tutor;
- Head of Phase;
- Head of Section; or
- DSL where the concern involves safeguarding.

Staff must report safeguarding concerns without delay.

A pupil does not need proof before reporting something that makes them feel unsafe or concerned.

Responding to Online-Safety Concerns

When an online-safety concern is identified, the School will determine whether it is primarily:

- a technical issue;
- a behaviour issue;
- a pastoral issue;
- a safeguarding concern; or
- a combination of these.

Where there is a risk of harm, safeguarding procedures take priority.
The School may:

- ensure immediate safety;
- preserve relevant evidence;
- restrict access to systems or devices;
- involve parents or guardians;
- provide pastoral support;
- apply behavioural consequences;
- involve IT;
- request removal of harmful content;
- contact online platforms;
- conduct a risk assessment;
- make a referral to SENNIAF;
- involve police or other appropriate Panamanian authorities; or
- take other proportionate action.

Devices, Searches and Evidence

Any search, inspection or confiscation of a device must comply with:

- applicable Panamanian law;
- the Behaviour Policy;
- approved searching and confiscation procedures;
- safeguarding requirements; and
- data-protection requirements.

Staff must not undertake intrusive searches of personal devices without appropriate authority.

Where potential criminal or safeguarding evidence may exist, staff must avoid actions that could compromise external investigation.

Online Incidents Outside School

The School may respond to online behaviour occurring outside School where it:

- affects the welfare or safety of a pupil;
- affects relationships or behaviour within School;
- involves members of the School community;
- disrupts the orderly operation of the School;
- has safeguarding implications; or
- otherwise has a material connection with School life.

Appropriate pastoral, behavioural, safeguarding or external-agency action may be taken.

Record Keeping

Online-safety concerns must be recorded through the appropriate School system.

Routine technical or behavioural incidents should be recorded through the relevant IT, pastoral or behaviour system.

Where an online concern raises a safeguarding issue or may constitute child-on-child abuse, it must also be recorded promptly on iSAMS Wellbeing Manager in accordance with the Safeguarding and Child Protection Policy.

Staff should avoid unnecessary duplication of sensitive safeguarding information across systems.

Records should be:

- factual;
- timely;
- proportionate;
- secure;
- appropriately restricted; and
- sufficient to show actions, decisions and follow-up.

Staff Training and Awareness

All staff receive online-safety training as part of safeguarding induction and regular safeguarding updates.
Training will include:

- current online risks;
- child-on-child online abuse;
- cyberbullying;
- online sexual harm;
- image sharing;
- generative AI;

- deepfakes;
- misinformation and disinformation;
- filtering and monitoring;
- professional boundaries;
- reporting procedures;
- preserving evidence appropriately; and
- local safeguarding escalation arrangements.

Staff training will be updated in response to emerging risks and significant changes in technology or guidance.

Monitoring and Review

The School will monitor online safety through:

- safeguarding records;
- behaviour data;
- IT incidents;
- filtering and monitoring reports;
- pupil voice;
- staff feedback;
- parent concerns;
- cyberbullying incidents;
- online sexual-harm concerns;
- emerging technology risks; and
- safeguarding audits.

The DSL, Head of School and appropriate IT and senior leaders will review significant trends and risks.

The policy will be reviewed annually or earlier where required by:

- changes in Panamanian law;
- changes to BSO standards;
- revisions to KCSIE or other relevant guidance;
- changes to Inspired Education requirements;
- significant incidents;
- material changes in technology;
- emerging AI risks;
- weaknesses identified through filtering and monitoring review; or
- lessons learned from practice.

Actions arising from review will be recorded and monitored.