



KINGSTONE ACADEMY TRUST

APPROVED DOCUMENT

Online Safety Policy	
Relevant School/s:	KHS and KTPS
Policy Officer:	Mr D Cook and Mrs A Preece
Approval:	Delegated
Date of Review:	October 2026
Next Review:	3 years or upon legislative change
Distribution:	Public, on website

1. Introduction

Kingstone Academy Trust is committed to a whole-school approach to online safety which protects, educates and empowers pupils, staff and the wider school community. Online safety is an integral part of safeguarding, not a stand-alone technical issue. This policy is read alongside the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct, the KAT Mobile Phones and Smart Technology Policy and our acceptable use agreements.

Our online safety practice is rooted in Courage, Kindness and Aspiration, and the expectation that everyone is Ready, Respectful and Safe, including in digital spaces. We recognise that technology may contribute to abuse, exploitation, grooming, bullying, radicalisation and other harms both on and off site.

The four categories of online risk:

Content – exposure to harmful, illegal or age-inappropriate material, including sexual content, hate, extremism, self-harm material, disinformation and AI-generated content.

Contact – harmful interaction with people or systems online, including grooming, coercion, impersonation and inappropriate interactions with AI companions or chatbots.

Conduct – unsafe or harmful behaviour, including cyberbullying, image-based abuse, sharing intimate images, harassment and discriminatory conduct.

Commerce – scams, gambling, phishing, fraud, aggressive advertising and financially exploitative activity.

All concerns are taken seriously. Staff must record and escalate concerns promptly; a behaviour response never replaces a safeguarding response where harm or risk is indicated.

2. Aims

Our aim is to provide clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach. This will involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

Education is the key to minimising the online risks to students. Responsible use of the internet, including online communication will be discussed through PSHE lessons and assemblies and form time sessions on appropriate online behaviour covering use in school and outside of school.

2.1 Online Safety

The Academy will work in partnership with parents, the DfE, the Police and our Network Service Provider to ensure systems to protect students are reviewed and improved. The Network Service Provider will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. If filtered websites need to be used by staff, they must inform the Network Service Provider to have them unblocked for a set period of time.

The Academy may invite external agencies such as the Police to support our e-safety programme, as a way of educating young people further about risk. For child perpetrators, this may involve work which focuses on respecting themselves and others.

The Academy will address the following:

- cyber bullying and sexting, and sharing of images with specific reference to our Anti Bullying Policy and Safeguarding Policy; the safe use of social media, including utilising privacy settings and the pitfalls of sharing personal information and photographs;
- the significance and consequences of their online behaviour, including digital footprints, legal sanctions and career prospects;
- online stranger danger, including how to recognise and report suspicious activity;
- Advice and guidance will be sought from The Child Exploitation and Online Protection Centre (CEOP, <http://www.ceop.police.uk/>) which brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse.
- Information will be provided to parents and carers via the school website which will address safety issues associated with social media and online communities. These articles outline the measures parents can take to educate and protect their children at home as well as informing them of the Academy's approach in terms of prevention and response to concerns.
- An e-safety audit will be carried out regularly. (see Appendix 1)

2.2 Guided Educational Use

- The curriculum requires students to learn how to locate, retrieve and exchange information using ICT.
- Curriculum internet use will be planned, task orientated and educational within a regulated and managed environment.
- Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Any user discovering unsuitable sites must report the address and content to a teacher or the DSL as appropriate

2.3 Internet Access

- The Academy will maintain an up-to-date record of all staff and students who are granted Internet access
- All Internet access is monitored and recorded using electronic means
- Inappropriate use of the Internet will be dealt with in accordance with each school's Behaviour Policy
- Pupils may only use approved email accounts on the Academy system
- Access in Academy to external personal email accounts will be blocked for all students
- Emails sent to an external organisation should be carefully written and authorised by a teacher before sending
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990

2.4 Academy Website Content

- The point of contact on the website will be the Academy address, email and telephone number.
- Use of photographs showing students and students' names will not be used on the website without parental consent (KAT is GDPR compliant)
- The copyright of all material will be held by the Academy or be attributed to the owner where permission to reproduce has been obtained

3. Roles & Responsibilities

It is the responsibility of all members of our school community, including teaching and non-teaching staff, governors, volunteers and students, to prevent and tackle e-safety issues. In line with the KAT Safeguarding Policy, all e-safety concerns should be shared at the earliest opportunity with the DSL or Deputy DSL and in any case before the end of the school day.

- Students will be instructed in responsible and safe internet use before being granted access
- Staff will receive training in Online Safety
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the Academy's Behaviour Policies, and Safeguarding Policy, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel (after consultation with HSCB and Police)
- Any complaints associated with the application of this policy will be dealt with through the Academy's Complaints Procedure

3.1 Board of Trustees

- Approve and review this policy at least annually and provide strategic safeguarding oversight.
- Ensure staff training, appropriate filtering and monitoring, effective cyber security and regular assurance reporting.
- Ensure an annual, documented review of filtering and monitoring, including tests on relevant devices and locations, and challenge gaps in provision.
- Ensure appropriate consideration is given to pupils with SEND and other additional vulnerabilities.

3.2 Heads of School and Senior Leaders

- Implement and communicate this policy; allocate clear safeguarding and technical responsibilities.
- Ensure pupils are taught online safety, concerns are acted upon and staff are trained.
- Commission and review regular filtering tests, monitoring reports and remedial actions with the DSL and IT support.

- Enforce a mobile phone-free school day in line with school procedures, considering justified individual exceptions.

3.3 Designated Safeguarding Lead (DSL) and Deputy DSLs

- Take lead safeguarding responsibility for online safety and understand the school's filtering and monitoring arrangements. The DSL is responsible for ensuring that technical staff are aware of what constitutes an e-safety concern which it would be necessary to report
- Review and triage Senso safeguarding alerts, including concerning keystroke patterns, and determine appropriate follow-up.
- Ensure concerns and decisions are recorded on MyConcern, with clear actions, owners, outcomes and follow-up.
- Consider referrals to children's social care, police, Prevent or CEOP where appropriate, following local safeguarding processes.
- Monitor themes and report significant risks, incidents and assurance issues to senior leaders and governors. The DSL will report regularly to the safeguarding governor on incidents of e-safety concerns and the subsequent actions and outcomes within the Academy.
- Support individual safety plans for pupils at increased risk and ensure online safety incidents inform curriculum and pastoral responses.

3.4 IT/network support and designated filtering lead

- Maintain and document the technical filtering solution, monitoring tools, system security and access permissions.
- Undertake and record tests of filtering effectiveness, including across relevant devices, users, networks and locations.
- Ensure appropriate alerts reach the safeguarding team without unnecessary delay and technical failures are escalated.
- Implement updates, backups, account security, access management and incident response in accordance with school procedures.
- Work with the DSL so appropriate safeguarding content is restricted without unjustifiably preventing legitimate learning.

3.5 All Staff

- Read and follow this policy, relevant safeguarding procedures and the Staff Code of Conduct. All staff are made aware that it is a breach of our Code of Conduct to have students as 'friends' on social media and that students and staff members should not communicate via personal telephone or email accounts.
- Staff must avoid photographing or recording pupils on personal devices unless explicitly authorised and managed in accordance with school policy.
- Staff are also made aware that their online posts which may bring the Academy into disrepute are not acceptable under the Staff Code of Conduct. which informs all staff of our expectations in terms of protecting their identity and upholding an online presence that is appropriate to their professional position.
- Maintain professional boundaries and use authorised systems when communicating with pupils.

- Record concerns without delay on MyConcern or immediately contact a DSL if urgent; follow contingency procedures if MyConcern is inaccessible.
- Do not investigate serious safeguarding incidents independently, circulate harmful images or promise confidentiality to a pupil.

3.6 Pupils, parents and carers

- Pupils are expected to use technology respectfully and safely, follow acceptable use requirements, report concerns and not seek to bypass school controls. Parents and carers are asked to reinforce online safety, support mobile-phone arrangements, report concerns and engage with school communications.
- Where the Academy receives information of a safeguarding nature concerning online activity which has taken place outside school, the Academy is equally committed to engaging with the students concerned and their parents to resolve the situation.
- Where we feel there is an ongoing risk to a young person, Children's Services and occasionally the Police, may be contacted to provide further support.

4. Teaching Online Safety

Online safety is explicitly taught and revisited through Computing, PHSE (personal, social, health and relationships education) which is delivered through the SPHERE programme at KHS, tutor activities, assemblies and relevant subject teaching. Learning is age-appropriate, inclusive, regularly updated and grounded in the risks young people actually encounter.

Evaluating online information: misinformation, disinformation, manipulated images, algorithms, persuasive design and online influence.

Healthy online relationships: consent, boundaries, cyberbullying, sexual harassment, coercion, grooming and reporting concerns.

Privacy and security: personal data, passwords, location-sharing, scams, phishing and safe digital footprints.

Artificial intelligence: deepfakes, fabricated media, privacy risks and the limitations of generative AI tools.

Wellbeing: managing screen use, harmful content and knowing when and how to seek trusted help.

4.1 Supporting pupils with additional vulnerabilities

Teaching and responses will be adapted for pupils with SEND, communication differences, social care involvement, experience of trauma or mental health difficulties. This may include explicit teaching, accessible resources, small-group intervention, trusted-adult check-ins and tailored risk assessments. Staff must not assume that a pupil understands online risk simply because they can use a device confidently.

5. Filtering and Monitoring

Kingstone High School uses Senso for keystroke monitoring and the identification of concerning activity. Senso alerts form part of the school's wider safeguarding system and are considered by the safeguarding team.

5.1 Operational expectations

- Relevant harmful or inappropriate content is filtered, with access restrictions proportionate to educational need.
- The safeguarding team regularly reviews monitoring alerts; urgent alerts receive prompt safeguarding triage.
- Significant alerts and resulting actions are documented on MyConcern, including the rationale when no further action is required.
- The DSL and IT staff complete a documented review of filtering and monitoring at least annually, with checks of effectiveness across relevant devices and locations.
- Filtering, monitoring and AI access are considered in risk assessments, including risks of bypassing controls through personal devices or mobile data.
- Staff report suspected gaps or failures immediately; the school records remedial actions and verifies that fixes work.

Monitoring is not a substitute for effective supervision, relationships, reporting routes or the teaching of online safety. Families will be given accessible information about the school's filtering and monitoring arrangements, including their limits.

6. Cyber Security and Data Protection

School systems are protected by proportionate technical and organisational controls, overseen by authorised IT leads. Measures include secure accounts and permissions, multi-factor authentication where appropriate, timely updates, malware protection, controlled installation of software, backups and incident response procedures.

Staff and pupils must safeguard login credentials and report phishing, lost devices, suspicious activity or possible data breaches promptly. Personal information is handled in line with the school's data protection policies and applicable UK GDPR requirements. Online learning platforms and new AI products are subject to appropriate safeguarding, privacy and technical review before use.

7. Working with Parents and Carers

Kingstone Academy Trust will communicate practical online safety advice through its websites, newsletters, parents' communications and targeted safeguarding messages. Communications will address emerging risks such as social media challenges, cyberbullying, exploitation, scams and AI-generated images.

Parents will be informed which online platforms pupils are asked to use, which school staff (if any) will communicate with them online, and how to report concerns. We will share information about filtering and monitoring systems and explain that no system can remove every risk.

8. Acceptable use Agreements

Pupils, staff, trustees and relevant volunteers are expected to comply with the school's applicable acceptable use arrangements. These cover school accounts, internet access, school-owned and personal devices, remote learning, communication, online content, privacy and security.

Unauthorised attempts to bypass filtering, access another person's account, capture or distribute harmful content, misuse AI tools or behave abusively online may result in safeguarding action, restorative work, proportionate sanctions or referral to external agencies, depending on the circumstances.

9. Mobile Phones, Smart Technology and Social Media

Please refer to the KAT Mobile Phone and Smart Technology Policy for detailed information.

9.1 Kingstone High School

Kingstone High School operates a mobile phone and smart devices free school day. Pupils who bring mobile phones to school must secure them in the school's magnetically locked Yondr pouches in accordance with the published school procedure. The detailed process for checking, locking, unlocking, damaged pouches, non-compliance and emergency contact is set out in the school's operational guidance and Behaviour Policy. Individual arrangements may be authorised by senior leaders where justified on medical, disability, safeguarding or other exceptional grounds and recorded appropriately.

9.2 Kingstone & Thruxton Primary School

The primary school has a ban on pupils' mobile phones unless there are explicit exceptions. Any authorised phone is handed to the office on arrival and collected by the adult at end of day.

9.3 Social Media

- Staff use school-approved systems for professional contact and must not use personal social media to communicate privately with pupils.
- Pupils must not use devices or platforms to bully, harass, threaten, impersonate others, create or distribute harmful imagery or expose others' personal information.
- Any suspected sexual image-sharing involving children must be referred immediately to the DSL; staff must not forward, save or routinely view such imagery.
- Parents are asked not to share identifying images, allegations or information about other pupils on public platforms, and to raise concerns directly with school.

10. Training and Staff Knowledge

Online safety forms part of staff induction and the annual safeguarding training programme, supplemented by staff briefings, updates and targeted guidance. Staff training addresses the four categories of risk, child-on-child abuse, AI-enabled risks, online radicalisation, the school's Senso arrangements, MyConcern reporting and urgent escalation.

DSLs and deputy DSLs maintain up-to-date knowledge through safeguarding training, professional updates and regular review of emerging risks. Staff must know that online and offline harms may overlap and that all concerns should be treated seriously.

11. Anti-bullying and Child-on-Child Abuse

Online bullying, sexual harassment, abusive messages, discriminatory content, non-consensual image sharing, threats and coercive behaviour are unacceptable. Such behaviour may occur outside school hours yet affect pupils' safety and wellbeing in school.

Staff follow the Child Protection and Safeguarding Policy, Anti-Bullying Policy and Behaviour Policy.

Safeguarding risks are assessed first; pastoral and behaviour responses may include protection and support for affected pupils, parent engagement where appropriate, restorative work, education and proportionate sanctions. Restorative conversations must never replace a necessary safeguarding response or expose victims to further harm.

Kingstone's Ready, Respectful, Safe expectations apply online. Incidents and patterns are reviewed to identify repeated targeting, discrimination, sexual harassment and broader safeguarding themes.

12. Reporting, Support and Associated Guidance

Reporting concerns at Kingstone

- Immediate danger or suspected serious crime: inform the DSL/head of school straight away and contact emergency services if necessary.
- Routine safeguarding concerns: report promptly through MyConcern and inform the DSL or deputy DSL as indicated by the level of risk.
- Technical control failure: alert the designated IT contact and DSL; record the issue and the action taken.
- Pupil disclosure: listen, reassure, avoid leading questions and do not promise secrecy; record facts accurately.

Trusted sources of help

- Child Exploitation and Online Protection (CEOP): <https://www.ceop.police.uk/Safety-Centre/>
- Report Harmful Content: <https://reportharmfulcontent.com/>
- NSPCC online safety: <https://www.nspcc.org.uk/keeping-children-safe/online-safety/>
- UK Safer Internet Centre: <https://saferinternet.org.uk/>

- Internet Matters: <https://www.internetmatters.org/>
- Childline: <https://www.childline.org.uk/>

Relevant policy and national guidance

- Keeping Children Safe in Education 2026 (DfE): <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- Mobile phones in schools (statutory guidance, updated June 2026): <https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools>
- Filtering and monitoring: core standard (DfE, updated September 2026): <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>
- Kingstone policies: Child Protection and Safeguarding, Behaviour, Anti-Bullying, Data Protection, Staff Code of Conduct, Acceptable Use and Prevent arrangements.

13. Review

- Methods to identify, assess and minimise risk will be reviewed regularly
- The Academy's IT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Files held on the Academy's network will be regularly checked
- Use of portable media such as memory sticks and CD will be reviewed regularly
- Downloading of unauthorised files will be prohibited, and where possible blocked

Appendix 1 KAT Online Safety Audit

Completed by:	Date:			
Policy	Yes	Partly	No	Evidence and Comments
The Academy has a set of policies which cover the following: Online Safety; Mobile phones; Use of Images; Social media; Bullying.				E safety Policy Safeguarding Policy School Rules Behaviour Policy
All policies are easily accessible to staff, pupils and parents.				Website and shared area
The online safeguarding policies have been adapted to incorporate the specific needs and requirements of the Academy.				
The policies have been reviewed and approved by SLT				Minutes
There is a nominated member of the Governing Body who has strategic oversight of online safety.				Safeguarding Trustee
Online safety policies are updated regularly to reflect changes in technology and national guidance (<i>at least annually</i>). Policies are also revisited following online safety incidents, to implement any lessons learnt.				On-going monitoring required
The Academy has a clear "Acceptable Use Policy" which outlines expectations for staff, parents, pupils and visitors regarding the use of technology in the Academy.				Visitor Policy Staff Code of Conduct
There are effective sanctions in place for anyone breaching the Academy's policies.				
The Academy regularly monitors and evaluates online safety approaches and mechanisms to ensure that the policy is consistently applied.				Alongside annual review of safeguarding policy

Responding to incidents	Yes	Partly	No	Evidence and Comments
Online safety is clearly identified as a safeguarding issue and concerns are managed in the same manner as other safeguarding issues.				
The DSL takes primary responsibility for online safety concerns that occur in the school.				
There are clear reporting mechanisms for pupils, parents/carers and staff, who have online safeguarding concerns.				Pastoral system My Concern reporting
There are specific procedures for responding to incidents of peer-on-peer abuse, including; Youth Produced Sexual Imagery (sexting) and cyber-bullying; in accordance with expectations in Keeping Children Safe in Education.				Safeguarding Policy
All members of the community are aware of the process for reporting concerns; all online safety incidents are passed to the DSL and/or Headteacher (<i>in cases of allegations against staff</i>).				
There are well developed strategies in place to ensure pupils feel safe and confident to report concerns, such as telling an adult if something online makes them feel worried, upset or uncomfortable.				
Online safety incidents are recorded and monitored by the DSL.				
Appropriate steps are taken to identify and protect vulnerable members of the community such as: looked after children, pupils with special educational needs or disabilities.				
All members of the wider community are aware of the				

process for reporting escalating concerns externally; all staff understand the Academy's whistleblowing procedure if they feel their concerns are not being managed appropriately.				
--	--	--	--	--

Infrastructure	Yes	Partly	No	Evidence and Comments
Access to the internet and Academy's network is secure.				
The Academy uses an appropriate internet service provider and implements appropriate filtering and monitoring.				
The use of Academy owned devices is monitored and there are robust procedures in place for responding to any concerns that are identified, in accordance with KCSIE and Prevent Duty.				
Personal data is managed securely online, in accordance with the statutory requirements of the GDPR 2018. All staff have due regard for data protection and understand the impact of data security. <i>E.g. Written parental consent for photos, encrypted emails, etc.</i>				
The Academy provides dedicated devices for taking photographs and making/receiving business communications <i>e.g. emails, phone calls, etc.</i>				
Members of staff do not use personal devices for business related activity. Emails, calls and other business related activity (<i>such as official social networking</i>) is done using the Academy's dedicated devices.				
All technology, apps and devices are subject to strict risk assessments prior to being introduced to pupils.				

Photographs or videos taken by the Academy are only shared in accordance with the Academy's Image Use Policy.				
---	--	--	--	--

Education and Training	Yes	Partly	No	Evidence and Comments
All members of staff (<i>including support staff</i>) receive regular and up-to-date online safety training. (<i>This is either stand-alone or incorporated within general safeguarding training</i>).				
The DSL has attended appropriate online safety/safeguarding training to ensure they have a higher level of knowledge regarding online safety issues.				
Members of staff receive regular updates regarding changes to policy and guidance or emerging online safety concerns.				
Staff induction training includes explicit reference to online safety, with regards to professional conduct and online reputation.				Code of Conduct
Staff role-model positive behaviours online by maintaining clear professional boundaries with parents and pupils. <i>I.e. keeping social network accounts private and not accepting pupils/parents as 'friends'.</i>				Code of Conduct
Pupils receive age appropriate, progressive and embedded online safety education throughout the curriculum.				
Pupils who are considered to be at increased risk online (such as children in care, children with SEND, children experiencing loss or trauma or children with mental health concerns) are provided with targeted or differentiated online safety education.				As identified.

The Academy has considered a range of strategies to support pupils in developing their own understanding of online safety and how to keep themselves and others safe. <i>For example, peer education.</i>				
The Academy engages with local and national events to promote positive online behaviour, e.g. Safer internet day and Anti-bullying week.				Needs to be embedded in the calendar
The Academy actively works to engage parents in their children's online safety education and signposts to support outside the Academy.				Opportunity for more to be put in place.
The Academy website includes online safety advice for pupils and parents and links to other organisations. There are also links to relevant online safeguarding policies and contact details of the DSL.				
The Academy offers training and support for parents and carers to ensure they understand online safety risks and their roles in safeguarding their children at home.				Information available via the website

Action Plan				
Key area for development		Resources, support or activity required	Date Completed	Signed
1				
2				
3				
4				
5				
6				