KINGSWAY COMMUNITY TRUST

KINGSWAY COMMUNITY TRUST

ONLINE SAFETY POLICY

February 2026

Online Safety Policy

Date: February 2026

Review date: Spring 2029

Aims

We aim to create a safe and secure environment in which all members of our Trust are protected in their use of technology. We aim to continually develop the curriculum, training, and management for ICT, digital technologies and online systems, enabling pupils' and adults alike in developing their ability to keep themselves and others safe when online.

The Trust is committed to meeting the Department for Education's six core digital and technology standards by ensuring that our digital environment is safe, secure, and well-governed. We maintain reliable, high-speed broadband, robust wireless coverage, and modern network switching to support effective learning and safeguarding. Strong digital leadership underpins our approach, ensuring clear roles and responsibilities for managing technology and online safety. We implement effective filtering and monitoring systems to protect pupils from harmful content, and we prioritise comprehensive cyber security measures to keep our data and community safe

Objectives

To achieve these aims, the Trust's objectives are to:

- Provide internet access expressly for educational use, which include carefully filtered material content appropriate to pupils, staff, volunteers and governors
- Maintain robust processes to ensure the online safety for the whole school community (pupils, staff, volunteers, parents and carers), through the application of acceptable use policies
- Deliver an effective approach to online safety learning, which educates the whole school community, and empowers children to protect themselves during online activity and use of devices
- To develop online safety learning, with units of work within the planned curriculum, including computing and PSHE
- To identify online safety concerns and incidents; intervening, addressing and escalating as appropriate
- Ensure all pupils learn how to be critically aware of the content they access online in all lessons and how to validate the appropriateness and accuracy of information
- Ensure that all pupils are able to communicate safely and appropriately, both with and without devices, both inside and outside of school
- Develop training and monitoring that ensures school systems and users are protected from accidental or deliberate misuse, that could put the security of the systems and users at risk
- Ensure pupils are supported in building resilience to online risks and communication by providing a safe environment for discussing issues or concerns; helping them to understand how they can influence and participate in decision-making.

By the age of 11 we aim for a child to be able to:

- Manage ICT and online systems effectively including individual accounts and shared files; promoting respect for others, including the safe use of equipment and technologies
- Evaluate and check the validity of content online, recognising bias and levels of accuracy in order to make informed decisions

- Recognise and avoid content online which may contain illegal, inappropriate or potentially harmful material
- Report content which is potentially illegal, inappropriate or harmful, to appropriate and designated individuals and authorities within and beyond schools
- Ensure that contact and communication, for example through emails and networking is always appropriate, to avoid being subjected to, or subjecting other users to, harmful online interaction
- Recognise the significance and impact of 'images' and 'videos' posted or published online, particularly of oneself and others
- Promote positive communication online, counteracting cyber-bullying, exploitation and extremism in all forms; dealing with incidents confidently and reporting them
- Employ safe practices with passwords, to prevent password sharing and identity theft
- Manage personal online behaviour and decrease the likelihood of harm in regard to sites used, privacy issues, disclosure of information, and health or well-being for example through managed time spent online

Statutory Requirements

This policy complies with the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on, Teaching Online Safety in Schools, Preventing and Tackling Bullying and Cyber-bullying (advice for headteachers and school staff) Relationships and Sex Education Searching and the DfE's guidance on protecting children from radicalisation.

The Trust's policy complies with existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, Equality Act 2010, Data Protection Act 2018 and Data (Use and Access) Act 2025. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

Reporting

Any identified online safety or e-safety concerns are to be reported to appropriate members of staff and referred to the Senior Leadership Team.

When misuses involve pupils, the Trust's ICT systems or internet, each school will follow the procedures set out in the Trust's Online Safety, and School Promoting Positive Behaviour Policies, including acceptable use policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will assess whether incidents involve illegal activity or content, or otherwise serious incidents, which require reporting to the police.

Roles and Responsibilities

The Executive Headteacher of Kingsway Community Trust has overall responsibility for safeguarding and on line safety and will ensure that:

- All staff should be included in Online safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal

- All staff are to read the Trust Staff IT Acceptable Use Policy and sign to acknowledge their understanding of the policy and give consent to adhere to it
- Monitoring and developing the whole school approach to e-safety and online safety
- A commitment to online Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- Ensure the use of data online and within digital systems meets the data protection act 2018, general data protection regulations (gdpr may 2018) and data (use and access) act 2025.
- In collaboration with the Finance Manager and IT Service Provider, purchasing and organising e-safety and online safety resources

The Trust Board will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on E-Learning & Online Safety within the school.
- Procedures are in place for dealing with breaches of online safety and security
- All staff and volunteers have access to appropriate ICT training.

The Head of School and or Designated Safeguarding Lead

- Ensuring that the policy is implemented, monitored and compliant with requirements and guidelines
- Addressing e-safety and online safety concerns and incidents, communicating with staff, parents and carers regarding breaches of AUPs, including action taken and future action
- Monitoring and evaluation of pupil achievement in the development and application of e-safety, online safety skills and practices
- Keeping up to date with recent developments in online safety
- Ensuring new teaching staff receive induction training, and additional training for staff where appropriate

PSHE Leads

- Monitoring and evaluating teaching and learning for e-safety and online safety, within a progressive curriculum
- Keeping up to date with recent developments in online safety
- Monitor the provision for e-safety and online safety within the wider curriculum, including assemblies, workshops, outside providers and the extended school curriculum
- Supporting staff with schemes of work and assessment
- Involvement of the wider school community in the promotion of online safety

Teaching staff:

Teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety and online safety procedures, through:

- Making e-safety and online safety a high priority, ensuring awareness of e-safety and ability to recognise online safety issues
- Managing the teaching and learning of online safety for pupils through the planned curriculum, including units of within the computing curriculum
- Compliance with the staff acceptable use policy (AUP)
- The understanding and implementation of the school's online safety policy
- Safe use of emails, and monitored use of pupils' email accounts
- Safe use of internet including use of agreed online systems and communication services
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such digital cameras and ipads
- Publication of pupil information and photographs, including safe use of website

- Promoting online safety, 'anti-bullying' and addressing cyberbullying, exploitation; reporting incidents to the online safety coordinator
- Seeking and implementing online safety and ICT training whenever required and applicable
- Being responsible for ensuring that conduct beyond the school boundaries, including conduct online, for example with social networking, does not compromise the reputation of the school, any members of the school community or the profession

The IT Service Provider is responsible for:

- Providing an appropriate level of security protection such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils and members of the Trust community are kept safe from potentially harmful and inappropriate content
- Ensuring that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring each school's ICTand online systems
- Work in blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Parents Carers and Pupils:

Parents and carers are expected to:

- Support the school in upholding the terms of the acceptable use policy and using advice to protect pupils and the whole community

Pupils are expected to:

- Adhere to the acceptable use policy
- Seek help from school staff if they have any concerns, and report online safety incidents
- Ensure that only school devices are used on the school site in accordance with the aup, supervised by school staff

Mobile Phones

The Trust does not permit children to use mobile phones and other mobile devices on site. Year 5 and Year 6 pupils may be permitted to have a mobile phone with them when they travel to and from school as long as it is handed at the school office on arrval at school.

- The phone is only carried by the designated child when the child travels to and from school on their own
- The mobile phone is switched off as the child enters the school site and the child does not use the phone on site at any time
- The mobile phone is handed in at the School Office to the school administrator on entry to the school
- The mobile phone is collected by the child at the end of the day
- The mobile phone will not be turned on again by the child until they leave the school premises
- The school reserves the right to withdraw this sanctioned carrying of a mobile phone to and from school, at any time in order to safeguard children and protect the wider school community

Mobile phones will not be used during lessons or formal times in school. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Promoting Positive Behaviour & Anti-Bullying.

Use of a personal mobile phone for taking photographs for the purpose of learning records is permitted with the instruction that photographs should be downloaded to the school drive and deleted from their personal device before leaving for the day. In the case of residential visits, photos should be downloaded on to the school drive and deleted from the personal device on return to school.

Equal Opportunities

The Trust is committed to providing equal opportunities for all pupils in their use of digital technology and online learning. We actively celebrate and promote diversity, ensuring every child feels valued, represented, and included in our digital environment. Online safety teaching and resources are designed to be accessible and respectful of all backgrounds, abilities, cultures, and identities.

Inclusion

This policy works in conjunction with the Promoting Positive Behaviour and Anti-Bullying, PSHE and Equalities Policies to develop achievement in IT, and safe practices and behaviours in pupils' use of ICT and online systems, enabling all pupils to access learning and achieve.

Parental Involvement

We are increasingly concerned about pupils' online activity at home, as issues that arise outside of school, often spill into the classroom and become difficult to manage. To help reduce these challenges, it is essential that parents have a strong understanding of online safety and are aware of what their children are doing online.

We encourage parental involvement in the following ways:

- Meetings with parents and carers, facilitating discussions and support regarding online access, the curriculum, provisions and resources for online safety
- Invitation to termly parents' evenings to discuss their child's progress and attainment, including behaviours and safe practice
- Parents are encouraged to engage in communication, either directly in personal or through the class email
- Online communication between teaching staff and families is encouraged through the use of the Google Classroom, using pupils' gmail accounts, with staff monitoring online and remote learning; communicate with families as appropriate, regarding remote learning and online safety
- Parents are informed by senior leaders regarding any breaches by pupils of the Acceptable Use Policy, including action taken and future action required (recorded in a secure log and communicated with parents and carers to address these concerns, by phone or meeting in person, as appropriate)
- School works with parents and carers to develop online safety at home and in the wider community, including workshops with parents, written communication, online resources available on the school website, and engagement with other agencies which have included training facilitated by the school

Safeguarding

Managing ICT/Online Systems

- Coordination of ICT and online systems, including agreed provisions, individual accounts and shared files, is carried out, managed and carefully monitored by the coordinators, alongside the SLT and IIT Service Provider
- The school promotes safe practices with passwords, in order to prevent password sharing and

identity theft.
- Only school devices with appropriate security and firewalls are used by pupils in school, and therefore children's own personal devices such as mobile phones are not permitted on site.

Evaluation of Online Material
- Chromebooks are used by pupils for research and work relating to agreed topics; recognising bias and levels of accuracy in order to make informed decisions.
- Age appropriate lessons, and discussions enable pupils to recognise and avoid content online which may contain illegal, inappropriate or potentially harmful material.
- Reporting of content which is inappropriate or potentially harmful is compulsory, by a child to the member of staff or adult supervising, and then by the member of staff to the SLT

Communication Including Emails and Networking
- Digital communication by adults and children in school is conducted and managed by the school, through (gmail) email accounts.
- Any other digital communication within school is through agreed sites, caches and systems, with unauthorised sites and social networks blocked by a sophisticated the Securly filtering system in school and on digital devices loaned to families beyond the school boundaries.

Cyber-bullying, Exploitation & Extremism
- Cyber-bullying like all forms of discrimination is not tolerated at this school. Pupils are encouraged to report cyber/online bullying to the Senior Leadership Team.
- The Trust promotes positive communication online, counteracting online bullying in all forms; and dealing with incidents, carefully reported, monitored and addressed

Filtering
Our Securly filtering generates an email to the Executive Headteacher/Head of School regarding suspicious search queries. This will pick up if students or staff have tried to search for anything that may be deemed as suspicious.

Our Securly filtering works by assigning a 'Category' to all known websites. These 'Categories' are then chosen as blocked or allowed by the Trust. In the event that a website is uncategorised it will be automatically blocked until either the IT Service Provider allows the site or it is categorised into an allowed Category. Securly maintains and updates the definitions for the Category. The Trust also maintains its own 'blocked' and 'allowed' lists of URLS and search terms so that URLs and terms can be allowed or blocked by the Trust regardless of Category.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Head of School and the Executive Headteacher. Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

Filtering methods will be selected by the school and will be age and curriculum appropriate.

Artifical Intelligence

Artificial Intelligence (AI) is a powerful new technology which has grown exponentially recently. There are a wide range of benefits in the use of AI, but due to the risks posed, and the risk assessments required, the pupils at Kingsway Community Trust do not currently have access to AI, and do not use AI tools directly in school or on school online systems.

Therefore, AI tools are used in school only by trained staff, for the benefit of pupils, through personalised

learning and report writing, monitored by senior leaders.

At Kingsway Community Trust we will only use the approved tool Gemini as this is part of our Google Suite. Teaching staff may use this system to create resources in order to enhance and support our existing broad and balanced curriculum, whilst other staff use them for effective report writing, proofchecked for accuracy. Resources created using Gemini are rigorously checked by teachers before being used with children, to ensure that they comply with our school curriculum and meet expected standards.

The school has risk assessed and checked online systems in line with safeguarding procedures; ensuring websites that fall under the category of AI do not pose additional risks to pupils and the school community, with appropriate filtering through the current firewall. This policy is subject to review with other school policies reviewed as required to ensure that AI is used beneficially and safely according to the following criteria.

Safeguarding Wellbeing and Safety:

- Use AI systems to prioritise the learning, physical, emotional, and psychological well-being and development ofpupils
- AI systems will not be used if there is risk of harm or distress topupils
- Regularly assess and monitor the use and impact of AI systems on pupil well-being and safety

Privacy and data protection:

- Staff **must not** input any personally identifying information into an AI system
- This includes names, photos, addresses, email addresses, medical information, behaviour notes or any combination of details that could identify an individual
- AI systems should only be used with fully anonymized or fictional examles when creating resources or draft content
- Do not upload or paste school documents containing any real personal data into an AI system (e.g reports, emails, assessment information)
- Only use the approved AI system for the Trust – remember many publicly available AI tools may store, reuse or learn from the data entered

Document Control	
Title	Online Safety Policy
Date	February 2026
Supersedes	February 2022
Amendments	
Related Policies/Guidance	• Trust Safeguarding Policy • Promoting Positive Behaviour and Anti-bullying policy • Staff IT Acceptable Use Policy • Adult Social Media Policy • Data Protection Policy
Review	Every 3 years

Appendix A

Student Acceptable Use Policy & Code of Conduct

I know that I must use the computers safely

- I know that the school can remotely monitor what I do on the computers.
- I will treat my username and password confidentially – I will not let anyone else use it, and I will not use theirs.
- I will be aware of my personal safety when I am communicating online, and will not share personal information about myself or others.
- I will tell a teacher immediately about any unpleasant or inappropriate material or messages on the computer, or anything that makes me feel uncomfortable when I see it.
- I understand that the school will look after me and my classmates and can help if anything happens online – even if I am using a computer at home.

I know that I must use the computers responsibly

- I understand that the computers are here for school work, and I will only play games on them or use them for personal use if I have permission.
- I will only upload pictures or videos from inside the school if I have permission.
- I understand that the school's security and Internet filter is there to protect me. If I need access to a blocked website, I will ask my teacher.
- I understand that I must not download or display inappropriate pictures or other material from the Internet.

I know that I must help look after the computers

- If I have a problem with my computer, I will tell a teacher immediately so that the problem can be fixed – I won't leave it broken for the next person.
- I will only use programs that are already on the school computer. If I need a new program, I will ask my teacher - I won't try to install it myself.
- I will not try to connect my own computer or mobile phone to the network.
- I will only change settings on the computer if I am allowed to do so – I won't try to change anything that might cause the computer to go wrong.
- I know that food should not be eaten whilst the laptops/iPads are out. Water bottles should be placed away from devices.,

I know that I must respect others when using the computers

- I will always treat others the same way I would want them to treat me – just as I would when not using the computers. I will not use the computers to harass or bully anyone.
- I will be polite online, and I will not use strong, aggressive, or inappropriate language. I appreciate that others may have different opinions.
- I will not take or distribute pictures or videos of anyone without their permission.

Appendix B

Type of Online abuse and cyberbullying

A range of elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online. These are identified in guidance provided by the Department for Education. Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world framework:

- Online relationships
- Privacy and security
- Online reputation
- Online bullying

Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal, such as forms of hate crime and blackmail. There are several forms of online abuse.

Cyberbullying
Cyberbullying is also known as online bullying. When someone experiences cyberbullying, it can be relentless as there is often no escape or safe space online and it can happen day or night.

Additionally, online bullies are often harder to trace and can also be anonymous. Surveys demonstrate that the two most common forms of online bullying experienced by 10% of all children from 10 years old were being called names, being sworn at or insulted and having nasty messages about them sent to them.

There are many ways that cyberbullies operate:

- Sending abusive or threatening messages
- Sharing or creating embarrassing photographs or videos
- Exclusion – intentionally excluding someone from a group chat, online activity or online game with the intent that the person sees that they are being excluded
- Shaming someone in a post or comment online
- Setting up a hate website directed to someone or a group of people
- Encouraging self-harming behaviours
- Creating a fake account or hijacking online identity to misrepresent them online
- Stalking someone online
- 'creeping' – where a person follows another's every move on their social media platforms but does not interact (although this is often done in secret)
- Withholding interactions online – someone can see that a person is interacting, commenting and liking on others' posts or activity online but is deliberately avoiding interacting with the victim
- Flaming – where a person known to the victim instigates an online fight through hurtful messages targeted at another using strong or harsh language usually in a public setting
- Trolling – sending messages/commenting on social network posts, online games or in chat rooms. The victim of trolling is not often known to the cyberbully
- Doxing or outing – this is when someone shares personal information online without the consent of the person to cause emotional harm or embarrassment. This can include screenshots of private messages or images
- Masquerading – where a bully adopts an online persona to bully someone that they know and protect their identity in the process.

Online Emotional Abuse
Many forms of online abuse overlap, and emotional abuse can and does play a part in any form of cyberbullying, as described above.

Emotional abuse can also include blackmail where someone is pressured into doing something that they do not want to do for fear of repercussions from the perpetrator. Such threats can include the threat of sharing images (including revenge porn) and the sharing of information (as described in doxing). Of course, the blackmail threats could also be offline and/or physical repercussions if a demand is not met.

Sexting
Sexting is where someone shares sexual content online usually via private messages. This can include sending nude or semi-nude images or videos or sexually explicit written content in a message. Sexting is often engaged in willingly by both participants who are of a similar age.

However, it can become online sexual abuse and/or sexual exploitation if someone receives unsolicited sexual content or is coerced into taking or sending sexual or nude images. This also applies if one of the participants is much older and/or is in a position of authority.

Sexual abuse
Sexual abuse can and does happen in person. However, sexual abuse can also be a form of online abuse. This occurs when someone is tricked or forced into any sexual activity. This can be tricking or forcing someone to watch, make or share a sexual video or view a sexual image, as well as taking part in sexual activities or sexual conversations online whether written, verbal or live streamed.

Of course, there is a definite overlap with sexting (as described above). Sexting becomes abuse when it is not solicited, when one person is much older or is in a position of authority or when sexting involves coercion. Online sexual abuse is often a precursor to physical sexual abuse.

Online sexual exploitation
Sexual exploitation is a type of online sexual abuse. This sexual exploitation involves manipulation. The perpetrator of the abuse deliberately manipulates or coerces their victim into participating in sexual activity including creating sexually explicit content and having sexual conversations.

Grooming
Grooming often takes place before online sexual abuse, as described above. It also happens in the build-up to real-life sexual abuse. Online grooming is the building of a relationship via the internet where trust and an emotional connection is established for the purposes of exploitation such as sexual abuse, trafficking and criminal exploitation, as well as radicalisation.

Children and young people can be groomed online by people that they know such as a professional, a friend or a family member as well as strangers.

Groomers gain the trust of their victims through a variety of means:

- Hiding their real identity online and pretending to be of a different sex or age.
- Sharing interests with their victims, often researching things that their victim is interested in to forge a connection.
- Giving advice and showing understanding.
- Paying lots of compliments and giving lots of attention. Sending or buying gifts.
- Taking them on trips once they have met in person.

Groomers can create trust in different ways by providing what they perceive their victim needs. It could be taking on a relationship role in a romantic sense or becoming a father figure. Trust could also be built in a mentor or ‘peer’ role or by someone who claims to be or is an authority figure.

A groomer then typically tries to isolate the victim from their friends or family, making them feel a sense of dependency on them. This gives the groomer power and control over the situation.

Groomers often introduce secrets or blackmail the child so that they feel guilty or ashamed. This is how groomers reduce their risk of being caught.

Children's feelings regarding online groomers are often complex. They often do not realise that they have been groomed and will struggle to believe it. They may continue to feel love, loyalty and even admiration for their groomer.

Online radicalisation
Children, young people and adult learners are at risk of accessing inappropriate and harmful extremist content online. This could include downloading or sharing terrorist material, which could be a criminal act.
The internet and social media make spreading divisive and hateful narratives easier. Extremist and terrorist groups and organisations use social media (for example, apps, forums, blogs, chat rooms) to identify and target vulnerable individuals.

Challenges
Online challenges acquire mass followings and encourage others to take part in what they suggest.

Content which incites
Knowing that violence can be incited online and escalate very quickly into offline violence