

KING EDWARD VII SCHOOL POLICY



Safeguarding Online

Date: September 2026

Approved: GB

Leadership Team Responsibility: CJ

Introduction

The need for School to have an Online Safeguarding Policy has arisen from rapid technological change and the exploitation or misuse of this technology.

This Online Safeguarding Policy applies to all members of the School community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of School digital systems, both in and out of the School.

Students and parents need to know that there are things that can be done to make it harder for these things to happen and this is the purpose of the Online Safeguarding Policy.

Despite the fact that many students will know more about new technologies than their parents (and often teachers), recent research suggests young people still regard the Internet as being safe. This policy aims to help tackle this complacency.

This Online Safeguarding Policy is closely linked to other policies including those for Artificial Intelligence, Consistent Conduct, Bullying and The Safeguarding and Child Protection Policy incorporating Self Harm. If a student is being bullied this will be tackled immediately by using the School's rigorous anti-bullying procedures.

King Edward VII School wants all staff and students to be able to use technological equipment effectively and safely in the knowledge that there are procedures in place to deal with situations arising from the abuse of these facilities.

The policy is informed by:

- Keeping Children Safe in Education 2026
- DfE Filtering and Monitoring Standards
- UK GDPR/Data Protection Act 2018
- Working Together to Safeguard Children
- Education for a Connected World Framework

Scope of the Policy

This policy applies to all members of the School community. King Edward VII School will deal with such incidents within this policy and associated behaviours and will inform parents / carers of incidents of inappropriate online safeguarding behaviour.

Current online risks:

- Cyberbullying
- Online abuse
- Grooming
- Child sexual exploitation
- Child criminal exploitation
- Sextortion
- Nude image sharing
- Radicalisation
- Misinformation and disinformation
- Livestreaming risks
- Online gambling
- Crypto-related scams

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Governing Board

- Governors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy.
- Senior management and governors are updated by the Headteacher / Online Safety Co-ordinator .

Online Safeguarding Coordinator (Designated Safeguarding Deputy – Online Safety Lead)

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with other agencies
- Liaises with the strategic manager
- Receives reports of online safety incidents
- Attends relevant governors' meetings
- Keeps abreast of current issues and guidance through organisations such as Sheffield LA, Learn Sheffield, National Crime Agency CEOP Education (Child Exploitation and Online Protection) and Childnet
- Arranges training and development for students
- Monitors the acceptable usage of the internet, with the Leadership Team (Assistant Headteacher - Safeguarding), therefore utilising the RM Safety and or Firewall settings in School and applying interventions as appropriate
- Encourages links between the online safety team of Learn Sheffield and the School
- Arranges assemblies at key points throughout the year.

Continuing Professional Development

Training will be offered as follows:

- All new staff receive online training as part of their induction programme, ensuring that they fully understand the Online Safeguarding Policy and acceptable use policies
- The Online Safety Coordinator will receive regular updates through training sessions and by reviewing guidance documents.
- The Online Safeguarding Policy and its updates will be presented to staff.
- The Online Safety Newsletter will be used to highlight concerns for online safety. These will be distributed monthly to parents, carers and staff.

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide students with high-quality Internet access as part of their learning experience
- The Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

- The School Internet access will be designed for student use and will include filtering appropriate to the age of students
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law
- Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This is addressed in PSHE and Computer Science lessons at Key Stage 3 and 4
- There is a robust and cohesive PSHE and Computing Curriculum that addresses the issues of online safety and educates our learners.

Managing Internet Access

Information system security

- The School's ICT system security will be reviewed regularly by the ICT Strategy Manager
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with Sheffield CYPD and the School in a timely manner.

- Monitoring Software – AB Tutor will be utilised by staff to monitor student usage and behaviour
- Smoothwall is used to monitor content and to keep students safe

E-mail

- Students may only use approved email accounts on the School system.
- Students must immediately tell a member of staff if they receive offensive emails
- In email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- Incoming emails should be treated as suspicious and attachments not opened unless the author is known
- The School considers how email from students to external bodies is presented and controlled
- The forwarding of chain letters is not permitted.

The School website and Managed Learning Environment (MLE)

- Staff or student personal contact information will not be published
- The Headteacher will take overall editorial responsibility and put in place systems to ensure published content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully so that individual students cannot easily be identified by a stranger or their image misused
- Students' full names will not be used anywhere on a School website associated with photographs; photographs without a name or name without a photograph can be used
- Written permission from parents/ carers will be obtained before photographs of students are published on the School website
- Wherever possible work should only be published with the permission of the student and parents/carers.

Social networking and personal publishing

- The School will control access to social networking sites and consider how to educate students in their safe use. Newsgroups will be blocked unless a specific use is approved.
- Students will be informed never to give out personal details of any kind which may identify them, their friends or their location.
- Students should not place personal photographs on any social network space without considering how the photo could be used now or in the future.
- Students will be informed on security and encouraged to set passwords to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others. Staff must not have current students as 'friends' or give their details to students for use on social networking sites.
- The use of social networking sites is prevalent and use by young people is not always positive. The Pastoral managers and Key Stage leads will work with external agencies to keep students safe. Advice may be made sought from the police if malicious and harmful content is shared.
- Sites used commonly by students include: Snapchat, Instagram, Tik Tok, Discord, Telegram, Reddit and gaming platforms with chat functionality.

Filtering

The DfE Technical Standards for Schools and Colleges states: "Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their School or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education 2026".

- Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.
- These standards help School and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- Members of the Leadership Team are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined
- the School manages access to content across its systems for all users and on all devices using the Schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for Schools and colleges.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
 - there is a clear process in place to deal with, and log, requests/approvals for filtering changes
 - There are regular checks of the effectiveness of the filtering systems .
 - access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with School policy and practice. The School has a no mobile device phone policy on the School grounds

Monitoring

The DfE Technical Standards for Schools and Colleges states:

“Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.”

- The School has monitoring systems in place, agreed by senior leaders and technical staff, to protect the School, systems and users: (Schools may wish to provide more specific details of their monitoring systems)

- The School monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
- Devices that are provided by the School have School-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices.
- where AI –supported monitoring is used, the purpose and scope of this is clearly communicated
- The School uses Smoothwall Internet Filtering to ensure that systems and students are protected
- If staff or students discover an unsuitable site, it must be reported to the ICT support team and the Designated Safeguard Lead
- Parents will be notified of safeguarding concerns or inappropriate usage and further sanctions and interventions put in place.

The Governing Board receives annual assurance regarding the effectiveness of filtering and monitoring systems.

Artificial Intelligence and emerging technologies

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in Schools: learner support, teacher support and School operations; ensuring all use is safe, ethical and responsible is essential.

- We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.
- We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.
- The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.
- The School acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The School recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet

data security standards before using them for work related to the School.

- Only those AI technologies approved by the School may be used. Staff should always use School-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The School will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The School will audit all AI systems in use and assess their potential impact on staff, learners and the School's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The School will support parents and carers in their understanding of the use of AI in the School
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially

important for external communication to avoid spreading misinformation.

- Recourse for improper use and disciplinary procedures. Improper use of AI tools, includes; creating images, audio or video hoaxes, deepfake pornography, breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action.
- If any student is found misusing AI to bully someone will be dealt with in accordance with our anti bullying policy.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in School is allowed
- The Leadership Team are aware that technologies such as mobile telephones with Internet access can bypass School filtering systems and present a new route to undesirable material and communications however the school has a no mobile phone policy.

The School recognises the risks posed by AI-generated deepfake imagery, audio and video, including their potential use in bullying, harassment, sexual abuse, reputational harm and misinformation. Any misuse will be treated as a safeguarding concern and addressed in accordance with the Safeguarding and Child Protection Policy.

Mobile phones and Smartwatches

Mobile phones and personal internet-enabled devices are prohibited on all school sites throughout the school day and will be confiscated if seen in accordance with the Consistent Conduct Policy.

- At Upper and Lower School mobile phones are prohibited to be used on site throughout the school day.
- The sending of abusive or inappropriate messages is forbidden
- The Consistent Conduct Policy outlines the rules of mobile phone usage in and around School.
- The use of smartwatches is forbidden in lessons and School.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and 2018.

- The School has taken the necessary steps to be fully GDPR compliant from 2018.

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT before using any School ICT resource
- The School will maintain a current record of all staff and students who are granted access to School ICT systems
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement
- Parents/carers will be asked to sign and return a consent form.

Assessing risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the School network. Neither the School or Sheffield CYPD can accept liability for any material accessed, or any consequences of Internet access
- The School will monitor ICT use to establish if the Online Safeguarding Policy is adequate and that the implementation of the Online Safeguarding Policy is appropriate and effective.

Handling Online Safeguarding Complaints

- Complaints of Internet misuse will be dealt with by the Safeguarding team, Key Stage Leads and the pastoral members of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a safeguarding or child protection nature must be dealt with in accordance with School safeguarding and child protection procedures. The safeguarding leads must be informed
- Students and parents will be informed
- Where appropriate, staff may seek advice from the Sheffield Safeguarding Hub, Police or the Safer Internet Team.

Incident Management

In this School, there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to

apply sanctions.

- all members and its wider community are encouraged to be vigilant in reporting issues in the confidence that issues will be dealt with quickly and sensitively, through the School's escalation processes
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online issues
- monitoring and reporting of online incidents will take place and contribute to developments in policy and practice in online safety within the School. The records are reviewed/audited and reported to the Leadership Team and governors. Parents / carers are specifically informed about online safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law
- we will use interventions as and when appropriate from internal and external professionals to teach students and parents of the risks associated with online usage
- we will distribute information to students via assemblies, Computer Science and PSHE lessons
- we will distribute information to parents on parent evenings and parental engagement programmes, workshops and through literature and presentations.

Community use of the Internet

The School will liaise with local organisations to establish a common approach to online safety.

Communicating Online Safety

Introducing the Online Safeguarding Safety Policy to students

- Online Safety rules will be posted in rooms where computers are used
- Assemblies will take place for each year group from Y7 to Y13
- Students will be informed that network and Internet use will be monitored
- A scheduled programme of training in Online Safety is delivered through Computer Science and PSHE
- Resources from CEOP (Child Exploitation and Online Protection Centre) will be delivered, and distributed to students in School.

- Additional personalised interventions may be given to some students by skilled staff, if identified by the Inclusion team.

Staff and the Online Safeguarding Policy

- All staff will be given the School's Online Safeguarding Policy and its importance explained
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and should follow clear procedures to report issues
- Staff should understand that telephone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting the support of parents and carers

- Attention will be drawn to the School's Online Safeguarding Policy in newsletters, the School prospectus and on the School website
- The School will maintain a list and website links of online safety resources for parents/carers
- A partnership approach to online safety at home and at School with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other attended events e.g. parents' evenings
- Parents will be requested to sign an online safety/Internet agreement as part of the Home School Agreement
- Parents will be encouraged to read and sign the School Acceptable Use Policy for students and discuss its implications with their children
- Information and guidance for parents/carers on online safety will be made available to parents/carers in a variety of formats
- Advice on useful resources, websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents/carers.