KING EDWARD VI SCHOOL
SHAKESPEARE'S SCHOOL

Online Safety Policy

Reviewed 6/2/24

Aim

The aim of the King Edward VI School Online Safety Policy is to safeguard members of our School community online in accordance with best practice and statutory guidance outlined in Keeping Children Safe in Education (KSCIE) and DfE publication: 'Teaching Online Safety in Schools' and guidance on filtering and monitoring. Our approach to online safety aims to address the following categories of risk:

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

Roles and Responsibilities

The Governing Body are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This review will be carried out annually by the Safeguarding Governor who is responsible for reporting significant online safety incidents to the Governing Body. Governors will support the School in encouraging parents and the wider community to become engaged in online safety activities.

The Headmaster is responsible for ensuring the implementation and day-to-day management of the policy and procedures. The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the School community and fostering a culture of safeguarding.

The Designated Safeguarding Lead (DSL) holds the lead responsibility for online safety, within their safeguarding role as defined in KCSIE. The DSL will:

- Promote an awareness of and commitment to online safety education and awareness within the School community.
- Be responsible for receiving, handling and recording reports of online safety incidents and deciding whether to make a referral by liaising with relevant agencies, including Prevent
- Be responsible for the filtering and monitoring systems and processes in place on School devices and School networks.
- To liaise with the Digital Strategy Lead to create a whole school approach to online safety

The Network Manager is responsible for:

- Implementing an appropriate level of security protection procedures, such as filtering and monitoring systems on School devices and networks, which are reviewed and updated annually to assess their effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online.
- Ensuring that the School's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

The Digital Strategy Lead will:

- Liaise with the DSL to create and implement a whole school approach to online safety.

1. Content

- The School manages access to content across online systems for all users on all School devices using filtering software that meets the standards defined in the DfE Filtering Standards for Schools and Colleges.
- Illegal content is filtered using a firewall that complies with Internet Watch Foundation URL list. Filtered content lists are regularly updated.
- There are established processes for users to report inappropriate content, recognising that no system can be 100% effective. The content accessed by users is monitored by the DSL using monitoring software. Inappropriate use is reported to the DSL and acted upon following the procedures outlined in the Behaviour and Safeguarding policies.
- If staff or students come across unsuitable online materials, the site must be reported to the Network Manager.

- The School will seek to ensure that the use of online materials by staff and students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Artificial Intelligence

- Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, students and parents may be familiar with generative chatbots such as ChatGPT and Google Bard.
- The School recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.
- Staff are made aware of the risks of using AI tools whilst they are still being developed.

2. Contact

Electronic Communication

- Students must immediately inform a member of staff if they receive an offensive electronic communication.
- Students must not reveal personal details of themselves or others in electronic communication or arrange to meet anyone without specific permission.
- Student to staff electronic communication must only take place via a School email address or Microsoft Teams and will be monitored.
- Incoming email must be treated as suspicious and attachments not opened unless the author is known.
- Students must seek authorisation for any email sent to external bodies when representing the School.

Published content and the School website

- The Headmaster takes overall editorial responsibility to ensure that content is accurate and appropriate.
- Photographs that include students will be selected carefully. The School will only use a student's first name with a digital image and will always ensure students are appropriately dressed.
- Permission is sought on image-taking, storage and publishing.

- Students are encouraged to tell the School if they are worried about any photographs that are taken of them.

Social networking and learning platform

- Students and parents will be advised that the use of social network spaces outside School brings a range of dangers for students.
- Students will be advised never to give out personal details of any kind which may identify them or their location. They are advised to use nicknames and avatars when using social networking sites.
- Students must not place personal photos or videos on the network without permission.

Mobile Phones

- Mobile phones must not be used during lessons without specific permission from the teacher in charge.
- The use of the camera functionality in any such device during the School day is forbidden unless with staff permission.

Remote Learning

- There is a separate Remote Learning Policy.
- The School may use live-streaming or video-conferencing services in line with national safeguarding guidance.
- Remote learning lessons must only take place via Microsoft Teams using an @kes.net account.
- Staff will understand and know how to set up and apply controls relating to student interactions, including microphones and cameras.
- Staff, students and parents will have a clear understanding of expectations around behaviour and participation.

3. Conduct

Acceptable use of the School network

- Staff must read the Staff Handbook before using any School network.
- Users of the School network must comply with the IT - Acceptable Use Policy.

Introducing the Online Safety Policy to Students

- A whole School approach to online safety is led by the Digital Strategy Lead.
- Appropriate elements of the Online Safety Policy are shared with students.

- Students will be informed that network and internet use will be monitored.
- Opportunities to gain awareness of online safety issues and how best to deal with them will be provided for students as part of the School's annual Online Safety Awareness Week.
- The whole School approach to online safety is based upon; culture, ethos, environment and partnerships with parents.
    - Culture
        - The risks posed by content, conduct, contact and commerce are embedded into the School Curriculum. Recommendations from the DfE Teaching Online Safety in Schools can be found in the PSHE, IT, Computer Science, Personal Development curricula.
        - As part of these curricula, students are informed of the specific processes required to report concerns and seek support in School.
    - Ethos
        - The School promotes a positive online ethos through assemblies, tutor group discussions, staff training and the Student Council.
        - Students can actively contribute to the development of the School's Online Safety approach through the Digital Strategy Group.
        - Staff receive regular training on Online Safety in line with the latest Keeping Children Safe in Education updates.
    - Environment
        - The School's online environment is closely monitored and filtered according to the principles set out in the DfE Filtering and Monitoring standards recommendations.
        - Students are informed of how their network usage is monitored during IT lessons and during the Digital Life Skills sessions in Sixth Form.
    - Partnerships with parents
        - The School seeks to proactively engage parents in School activities that promote the agreed principles of online safety.
        - Parent Online Safety Evenings take place at the beginning of each key stage in Lower, Middle School and Sixth Form.
        - A Parent Information Evening for Year 11 parents is held for those whose sons are moving into Sixth Form to inform them of the BYOD policy.

Enlisting Parents' Support

- Parents' attention will be signposted to this policy on the Parent Portal.

- Parents will be provided information on online safety as part of the annual Online Safety Awareness Week. Parent online safety information meetings are held in Year 7, 9 and 12.
- Parents are required to sign the Home-School Agreement when they register their child with the School. Sixth Form students are required to sign the Sixth Form Agreement.

Cyberbullying

- Cyberbullying involves the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. It differs from other forms of bullying in that it can invade the home and personal space, be anonymous, attract the attention of a wide audience, and be characterised by the difficulty of controlling electronically circulated messages. It can, and does, affect both students and staff. Cyberbullying will often originate off site. The School is empowered by law to regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff.

Typical examples of cyberbullying include:

- Threats and intimidation using mobile phone, texts, email, comments on websites or social networking sites or message boards.
- Harassment or stalking. Repeated, prolonged, unwanted texting whether offensive or not is a form of harassment. Monitoring a person's online activities, sometimes referred to as cyber-stalking. Using public forms, such as message boards, chatrooms or social networking sites to repeatedly harass, or to post derogatory or defamatory statements in order to provoke a response from the target.
- Vilification/defamation through posting upsetting or defamatory remarks about an individual online, or name-calling using a mobile device.
- Ostracising/peer rejection/exclusion/inciting hatred, using social networking sites to exclude someone.
- Identity theft, unauthorised access and impersonation, through accessing someone else's account by finding out or guessing their username and password information.
- Hacking somebody's account in this way is illegal under the Computer Misuse Act 1990. Unauthorised access to somebody else's account can lead to:
    - Posting private information on public sites, or via email in order to harass or humiliate.
    - Deleting information.
    - Impersonation. There have been cases where a bully has sent out nasty messages to everyone on a student's contact list, and images and contact details have been posted to public sites with invitations to contact them.

- Sending/forwarding Images. Once pictures are made public it becomes very difficult to contain them. They can be circulated via phones, email and postings to social networking sites. Creating, possessing, copying or distributing images of children and young people under the age of 18 which are of an indecent or sexual nature is illegal under the Protection of Children Act, 1978. Such pictures are illegal even if they were consensual and police involvement will be sought if considered appropriate.
- Manipulation, for example, putting pressure on someone to reveal personal information.
- Users of Social Networking Sites may post a lot of detailed and personal information about themselves and their friends. It can then be misused. Such sites can be abused in a number of ways:
    - Nasty comments may be posted.
    - People might use their own sites to spread rumours or make unpleasant comments, or post humiliating images or videos.
    - Fake profiles are also common in order to pretend to be someone else.

4. Commerce

Risks such as online gambling, inappropriate advertising, phishing and/or financial scams are mitigated via the filtering and monitoring systems within the School.