KING EDWARD VI SCHOOL
SHAKESPEARE'S SCHOOL

E-Safety Policy

Reviewed 09.11.22

The aim of the King Edward VI School E-Safety Policy is to establish best practice, primarily to safeguard children whilst using IT systems. The E-Safety Policy relates to various other policies including those for bullying and safeguarding. The E-Safety Policy has been written by the School, building on best practice and government guidance and will be reviewed regularly.

Why Internet and Digital Communications are Important

- The internet is an essential element of 21st century life for education, business and social interaction. The School has a duty to provide students with quality internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students
- Internet access is provided and includes filtering appropriate to the age of students
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use. They will be required to agree to the School's IT- Acceptable Use Policy
- 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 shown how to publish and present information appropriately to a wider audience.

Evaluating Internet content

- The School will seek to ensure that the use of internet derived materials by staff and by 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
- Students will be encouraged to report unpleasant internet content.

Information System Security

The School's security strategies are discussed with external agencies. The School IT systems security is reviewed regularly and virus protection is systematically updated.

Electronic Communication

Students and staff may use web-based e-mail accounts on the School system as well as through the learning platforms.

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 and will be monitored.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The School will be authorise how e-mail from students to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

Published content and the school web site

- The Headmaster or nominee takes overall editorial responsibility and 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
- Parents will be clearly informed of the School policy on image taking and publishing, both on School and independent electronic repositories
- All 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 on the network without permission

Managing filtering

- The School will work in partnership with outside agencies to ensure systems to protect students are reviewed and improved
- If staff or students come across unsuitable on-line materials, the site must be reported to the Network Manager
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

Managing emerging technologies

Mobile phones and associated cameras 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 supervised by a member of staff or with express staff permission.

Protecting personal data

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

Authorising Internet access

- All staff must read the Staff Handbook before using any School IT resource
- Visitors must comply with the IT - Acceptable Use Policy

Assessing risks

- The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer. The School cannot accept liability for the material accessed, or any consequences of internet access
- The School will audit IT use to establish if the E-Safety Policy is adequate and that its implementation is appropriate and effective

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headmaster
- Complaints of a safeguarding nature must be dealt with in accordance with School safeguarding procedures
- Students and parents will be informed of the complaints procedure
- Students and parents will be informed of consequences for students misusing the internet

Community Use of the Internet

All use of the School internet connection by community and other organisations shall be in accordance with the School's E-Safety Policy.

Introducing the E-Safety Policy to Students

- Appropriate elements of the E-Safety Policy will be shared with students
- Students will be informed that network and internet use will be monitored
- Opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for students as part of the School's annual E-Safety Awareness Week

.**Enlisting Parents' Support**

- Parents' and carers attention will be drawn to the School E-Safety Policy on the School Website
- Parents and carers will be provided information on e-safety as part of the School's annual E-Safety Awareness Week
- The School will ask all new parents to sign the parent /pupil agreement when they register their child with the School

Cyberbullying

Definition and Scope

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.

Forms of Cyberbullying

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, chat-rooms 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 pupil's buddy 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 taken for ‘fun’ or by ‘willing’ parties
- 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 fairly common in order to pretend to be someone else.

Dealing with Cyberbullying

There are no excuses for cyberbullying; students need to be aware that their actions have severe and distressing consequences and that participating in such activity directly or indirectly will not be tolerated. The School will implement the following procedures:

- The School network will be monitored and examples of inappropriate emails received or sent, and inappropriate website content will be captured with user details, date and time, and machine IP address and such material will be used as evidence
- Any reported incidents of cyber-bullying will be investigated
- Internet service providers, mobile phone companies and social networking sites may be contacted to obtain relevant user information as appropriate
- Police involvement will be sought if considered appropriate
- Once the person responsible for the cyberbullying has been identified appropriate sanctions will be applied consistent with the School’s Behaviour Policy. Additional action may include disabling School network access (either on a temporary or permanent basis) and/or removing the right to use a mobile phone on the School site. The defence that “someone else used my account” will not be accepted without proof