KING EDWARD VII SCHOOL POLICY

Online Safeguarding Policy

Document Adopted by Governing Body
Date: July 2022 Signed (Chair): Print Name: Peter Dickson Leadership Team Responsibility: Catherine Jackson

King Edward VII School Online Safeguarding Policy

Introduction

The need for School to have an Online Safety Policy has arisen from rapid technological change and the exploitation or misuse of this technology. At the worst level this can be illegal online activity where adults deceptively befriend young students. At School, it is more likely to be cyberbullying where social networking sites such as Facebook and WhatsApp or even emails are used to bully another student. The School also wants to do as much as is practically possible to prevent offensive material appearing on the network. 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 that up to 60% of young people still regard the Internet as being completely safe. This policy aims to help tackle this complacency.

This Online Safeguarding Policy is part of the annual School Improvement Plan It is closely linked to other policies including those for ICT, Consistent Conduct, Bullying and Safeguarding and Child Protection Policy incorporating Self Harm and Online Safety. 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 computer equipment effectively and safely in the knowledge that there are procedures in place to deal with situations arising from the abuse of these facilities.

1 Writing and reviewing the Online Safeguarding Policy

The Online Safeguarding Policy is to be reviewed by the ICT Strategy Group at least every two years. The Assistant Headteacher and Online Safety Coordinator responsible for the policy, need to ensure that the policy works and that it is widely available and understood. The ICT Strategy Manager is responsible for implementing the strategy and monitoring its effectiveness across the School network.

Teachers responsible for safeguarding and child protection must be fully aware of the Online Safeguarding Policy.

This Online Safeguarding Policy has been written by the School, using Sheffield Safeguarding Board Guidance and in conjunction with other schools and external

advice and support. It has been agreed by the Leadership Team and approved by governors.

Scope of the Policy

This policy applies to all members of the School community who have access to and are users of IT systems, both in and out of the building.

The Education and Inspections Act 2006 empowers leaders, to such extent as is reasonable, to regulate the behaviour of students when they are off the School site. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of the School. The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate online safeguarding behaviour.

This policy, supported by the School's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole community. It is linked to the following mandatory policies: Safeguarding and Child Protection Policy incorporating Self Harm and Online Safety, Acceptable Use Policy, Cameras and mobile phones, Health and Safety, Home–School agreements, and the Consistent Conduct (including the anti-bullying) Policy, CCTV and the PSHE Raising Achievement Plan.

Governors

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 Safeguarding Co-ordinator.

Online Safeguarding Coordinator

- 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, Becta, CEOP (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 Sheffield and the School
- Arranges assemblies at key points throughout the year.

Continuing Professional Development

Training will be offered as follows:
- All new staff should 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.

2 Teaching and learning

Why the Internet and digital communications are important
- 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 IT lessons at Key Stage 3 and 4

3 Managing Internet Access

Information system security

- The School 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.

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
- 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 advised 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 should be advised 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 are strongly advised not to have current students as 'friends' or give their details to students for use on social networking sites.

Managing filtering

- 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
- The ICT Strategy Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Parents will be notified of safeguarding concerns or inappropriate usage and further sanctions and interventions put in place.

Managing videoconferencing

- Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet
- Students should ask permission from the supervising teacher before making or answering a video conference call
- Videoconferencing will be appropriately supervised according to the students' age.

Managing emerging technologies

- 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 phones with wireless Internet access can bypass School filtering systems and present a new route to undesirable material and communications
- Games devices such as Playstations and Xboxes have Internet access which may not include filtering. Care is required in any use in School (in a lunchtime club, for example) or other official location.

Mobile phones and Smartwatches

- The use of mobile telephones or any other electronic or digital device is banned in the building at Lower School. Such devices will be confiscated if seen in line with the Consistent Conduct Policy
- At Upper School, mobile telephones and other electronic or digital devices can only be used at designated times in line with the School's Consistent Conduct Policy
- At Upper School mobile phones must not be used for phoning or texting during lessons.

- The sending of abusive or inappropriate text messages is forbidden both in School and outside School
- The use by students of cameras in mobile phones for good educational reasons is allowable under staff supervision and in line with the Consistent Conduct Policy. The taking or sending of inappropriate photographs is forbidden in both inside and outside of the School premises.
- The School recognises that the nature of mobile phones is changing fast and their future use as all-in-one communication centres (including data storage) will necessitate regular review.
- 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.
- The School has taken the necessary steps to be fully GDPR compliant from 2018.

4 Policy Decisions

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 Safeguarding 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.

5 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.

Staff and the Online Safety 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.

C O Daly, D Kavanagh, C Jackson

September 2022