E-Safety Policy

Owner: J Dunbar
Approved: SLT on 2nd May 2018
Review: May 2021

1.0 Statement of Intent

1.1 At The Kingsway School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

1.2 Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

1.3 Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1.4 The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

2.0 Legal Framework

2.1 This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

2.2 This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

3.0 Use of the internet

3.1 The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

3.2 Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

3.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

4.0 Roles and responsibilities

All staff:

4.1 It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

Network Manager:

4.2 The Network Manager is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils. This is to be monitored by the Safeguarding Lead.

4.23 Ensure the network has adequate virus protection and security protocols, e.g. password protection and encryption.

Safeguarding Lead:

4.3 The Safeguarding Lead is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.

4.4 The Safeguarding Lead will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

4.5 The Safeguarding Lead will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher.

4.6 The Safeguarding Lead will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

4.7 The Safeguarding Lead will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

4.8 The Safeguarding Lead will review and amend this policy, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

4.9 The Safeguarding Lead responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

Headteacher:

4.10 The Headteacher is responsible for ensuring that Safeguarding Lead and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

Governing Body:

4.12 The Governing Body will hold regular meetings with the Safeguarding Lead to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

4.13 The Governing Body will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

All Staff:

4.14 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

4.15 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

All Staff and Pupils

4.16 All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement.

Parents:

4.17 Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

5.0 E-Safety Education

5.1 Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and

the validity of website content.

- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

5.2 Educating staff:

- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- The Safeguarding Lead will act as the first point of contact for staff requiring e-safety advice.

5.3 Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

6.0 E-Safety Control Measures

6.1 Internet access:

- Our Acceptable Use Agreement is displayed for pupils every two weeks, and pupils are required to review and agree to the agreement to continue use of the school network.
- Pupils' activity is continuously monitored by the Safeguarding Lead.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to prevent risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- All school systems will be protected by up-to-date virus software.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the Safeguarding Lead for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

6.2 Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate profanity, viruses and malware.

6.3 Social Networking:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught.

6.4 Images:

- Students are not permitted to take images on personal devices during the school day
- Staff may take images if required by their role on personal devices provided no individuals are within frame
- Staff may take images if required by their role on school devices for the purposes of assessment, training or other legitimate need. These images must be destroyed once they are no longer required.

7.0 Cyber bullying

7.1 For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

7.2 The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

7.3 Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

7.4 The school will commit to creating a learning and teaching environment which is free from

harassment and bullying, ensuring the happiness of all members of staff and pupils.

8.0 Misuse by Pupils:

8.1 Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet may have their internet privileges removed.

8.2 Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy.

9.0 Misuse by Staff:

9.1 Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.

9.2 The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy, and may decide to take disciplinary action against the member of staff.

Appendix A: Student Acceptable Use Agreement

At The Kingsway School we understand the importance and benefits of emerging technologies for student's learning and personal development. However, we also recognise that safeguards need to be in place to ensure we are all kept safe.

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school equipment.
- I will only log on to the school network/ learning platform with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of a teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Appendix B: Staff Acceptable Use Agreement

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly, and will be reported to the headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. Using technology in school

    - I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the Network Manager.
    - I will only use the approved email accounts that have been provided to me.
    - I will not share sensitive personal data with any other pupils, staff or third parties.
    - I will ensure that any personal data is stored in line with the Data Protection rules.
    - I will delete any chain letters, spam and other emails from unknown sources without opening them.
    - I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
    - I will only use the internet for personal use during out-of-school hours, including break and lunch times.
    - I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
    - I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
    - I will not install any software onto school ICT systems unless instructed to do so by the Network Manager or Headteacher.
    - I will only use recommended removable media, and will keep this securely stored.
    - I will provide removable media to the Network Manager for safe disposal once I am finished with it.

2. Mobile devices

    - I will only use school-owned mobile devices for educational purposes.
    - I will only use personal mobile devices during out-of-school hours, including break and lunch times.
    - I will ensure that mobile devices are either switched off or set to silent mode during school hours
    - I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from my line manager before any school-owned mobile device is used to take images or recordings.

- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the Network Manager.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access social networking sites, unless it is beneficial to the material being taught
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over social networking sites.
- I will ensure that I apply the necessary privacy settings to my social networking sites.
- I will not publish any comments or posts about the school on my social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Training

- I will ensure I participate in any e-safety or online training offered to me
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

5. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the pupil's pastoral Head of Year or Headteacher for staff
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me in if I breach this agreement.

DOCUMENT END