ONLINE SAFETY POLICY

Introduction

Computer technology has transformed the process of teaching and learning in School. It is a crucial component of every School subject and is taught as a subject in its own right. Classrooms are equipped with projectors and computers. There are a number of computer suits in the School, and pupils may use the machines in these rooms to complete their School work. Boarding houses are equipped with computers and network points. Members of the School have access to a secure, filtered and monitored network and Internet, including WIFI. The filtering and monitoring systems are managed by the IT Manager and the School's e-Safety team monitor and act upon breaches.
However, the use of this technology involves many risks and it is important that we are all able to deal with unwanted behaviour/attention. It is also important that we are respectful to other online users. This is a supplementary policy to the *IT Acceptable Use Policy*.

During Computing lessons pupils are taught about the dangers of online communication and how to deal with any issues. Online safety posters are displayed in all computer suits and offer guidance and independent contact details.

Role of technical staff

In taking account the speed at which technology advances, we recognise that we need to educate pupils to behave responsibly when 'online'. This aspect is a role for all staff. Our technical staff has a key role in maintaining a safe technical infrastructure and in keeping abreast with the rapid succession of technical developments. He/She is are responsible for the security of our network and its data, and for training our staff when using computing technology. He/She monitors the use of the internet and e-mails and will report inappropriate usage, to the E-Safety Group, our Designated Safeguarding Lead and, as appropriate, to the Headmistress.

Role of Designated Safeguarding Lead

The School recognises that online safety is a safeguarding issue. The Designated Safeguarding Lead has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. He/she works closely with the Educational Safeguarding Advisory Team (ESAT), Local Safeguarding Children Board (LSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of our School. All staff members are aware of their pastoral responsibilities in relation to online issues. The Designated Safeguarding Lead oversees the School's comprehensive Personal, Social, Health and Economic Education (PSHEE) programme on online. The Designated Safeguarding Lead ensures that pupils are educated in the risks and the reasons why they need to behave responsibly online. It is his/her responsibility to handle allegations of misuse of the internet.

Misuse: statement of policy

The School will not tolerate any illegal material, and will report illegal activity to the Police and/or the ESAT or LSCB. If a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We shall impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

Involvement with parents and guardians

The School will work closely with parents and guardians in promoting a culture of online safety. We shall always contact parents if we have any concerns about their children's behaviour in this area, and we hope that parents will feel able to share any concerns with us. We recognise that not all parents and guardians may feel equipped to protect children when they use electronic equipment at home. We therefore may arrange evening events for parents where the Head of Computing advises about the potential hazards of this advancing technology and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. Imminent dangers will be explained through email as would updates on online safety.

Charter for the safe use of the internet and electronic devices at School

Children and young people need to be empowered to keep themselves safe. This is not a top-down approach. Children will explore and take risks. Online safety is a whole-school responsibility, and staff and pupils have adopted the following charter for the safe use of the internet inside the School:

Cyber-bullying

- Cyber-bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our School's *Anti-Bullying Policy* describes our preventative measures and the procedures which will be followed when we discover cases of bullying
- Proper supervision of pupils plays an important part in creating a safe environment in School: everyone needs to learn how to stay safe outside School
- We value pupils equally. It is part of the ethos of our School to promote considerate behaviour and to value diversity
- Bullying and harassment in any form should always be reported to a member of staff or the Anti-Bullying Ambassadors. It is never the victim's fault, and he/she should not be afraid to come forward

Treating other users with respect

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the School's *Behaviour Management Policy*
- We expect a degree of formality in communications between staff and pupils, and we do not expect pupils and teaching staff to communicate informally with each other by texting or mobile telephone. (Use of ICT, Devices etc….) Our policy on out-of-school visits (*Educational Visits Policy*) explains the circumstances when communication by mobile telephone may be appropriate. Teachers and current/former pupils should not communicate at all via social networking sites (See also Staff behaviour and code of conduct policy including staff dress code)
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated as outlined in the School's *Anti-Bullying Policy*.
- The School is strongly committed to promoting equal opportunities for all
- All pupils are encouraged to look after each other and to report to staff any concerns about the misuse of technology or any other worrying issue

- The use of cameras on mobile telephones is outlined in our policy: *Use of ICT, Mobile Phones Cameras and Other Electronic Devices: Taking, Storing and Using Images of Children.*

Keeping the School network safe

- All users adhere to best practice regarding e-teaching and the internet.
- Certain sites are blocked by our filtering system, and our Network Manager monitors pupils' use of the network
- The Network Manager uses software to monitor e-mail traffic and blocks SPAM and certain attachments through a filtering system
- Pupils in Years 5 and above are issued with their own personal School e-mail address
- Access is via a personal LOGIN, which is password protected
- We give guidance on the reasons for logging off and for keeping all passwords secure
- Access to sites such as web-based email and social media is not allowed on the School's network, except for limited access for boarding pupils
- Anti-virus protection is installed, which is managed by the Network Manager
- Any member of staff or pupil who wishes to connect a removable device to the School's networked hardware agrees to comply with the school's *Data Encryption Policy*

Promoting safe use of technology

Pupils of all ages are encouraged to make use of the online resources that are available from the following sites:

- UK Council for Child Internet Safety (www.education.gov.uk/ukccis)
- Childnet International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyber-bullying (www.cyberbullying.org)
- Bullying UK (www.bullying.co.uk)
- ThinkUKnow (www.thinkuknow.co.uk)

Pupils are taught during discrete Computing lessons throughout Key Stages 1, 2 and 3 and are advised in PSHEE, assemblies, form time and take part in the annual Safer Internet Day. Below are suggestions that are based on advice provided by respected sources in the field:

Advice for the safe use of mobile phones and digital devices

- Be careful to whom you give your mobile phone number and never post it on websites
- Never return a call or text message to a number you do not know
- Never reply to texts saying you have won prizes as these are usually based around premium rate numbers and may cost a lot
- If you are using text chat, make sure your username does not give away your real name
- If you receive abusive text messages, keep them, you do not have to read them and when the time comes to take action, these messages can be used as evidence
- If you receive abusive text or chat messages, ask for help from a parent, your Form Tutor, the School Nurse, the School Counsellor or any trusted adult
- You can also contact your mobile phone or social media provider or report the event to an online organisation such as CEOP

- Remember, by forwarding a text, email, photo, video, etc you may be making a problem worse or you could be unwittingly involving yourself in bullying -you may even be breaking the law
- Be careful with the language you use when texting, using email, instant messenger etc as the person receiving your message may be offended by your choice of words or even misinterpret what you say and take offence

Advice for the safe use of the internet

- Always make up usernames that are not linked to your real name
- Never agree to meet anyone you have met online unless you are sure they are who they say they are, you have discussed it with your parents and you meet them in a public place in daylight
- Remember that many people in chatrooms and on social networks are not who they say they are
- Always avoid posting personal information on websites such as social networking sites and in blogs
- Information, such as your real name, address, phone number, email address, School, postcode and photos of you in your School uniform can be used to trace you or use your identity
- Be careful about putting photos of yourself or friends on websites
- Never send photos to someone you have met only online
- Avoid webcam chats, such as Skype, with people you do not know
- Do not respond to emails from people you do not know
- If creating online accounts, use your School email address, as this is filtered and does not contain your real name
- Do not respond to any abusive emails
- If you receive any abusive emails, keep them
- Your passwords are very important; never share them, even with friends
- Remember that passwords are more secure if they contain a combination of numbers and letters (please refer to the School's *Password Policy)*
- Learn how to block people on email or websites
- If someone sends you inappropriate mail, block them
- Remember to contact the site administrators if you want something to be removed from a website

Considerate use of electronic equipment

- Mobile telephones and other personal electronic devices should be switched off and stored securely during the School day, unless they are being used for educational purposes
- They may be used during break time, lunch times and in boarding houses after School; they should not be visible outside of form rooms
- Personal electronic devices being used during the School day will be confiscated by staff and passed to the relevant Heads of Section or Deputy Head until the end of the School day

- Sanctions may be imposed on pupils who use electronic equipment without consideration for others

We expect all pupils to adhere to this charter for the safe use of the internet. Copies are made available to all pupils and their parents, and we may impose sanctions for the misuse or attempted misuse of the internet, mobile telephones and other electronic devices.

In relation to the Prevent Duty

- Staff receive training to recognise the signs of radicalisation and the duty to report concerns
- Protection is provided for pupils by the School's filtering software, awareness for pupils through the Personal, Social, Health and Economic Education (PSHEE) programme and careful logging of concerns
- Risk assessments are conducted for pupils, staff and visitors as needed
- The danger of radicalisation (and well as grooming from other sources) is taught during Computing lessons.

081119