Ellis Guilford School

E-Safety Policy
September 2017/18

Review July 2020/21

1. Rationale

"For young people ICT is not a novelty but the way they engage with their world - 21st century culture" (Becta – eSaety Guide)

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The use of New Technologies can introduce a number of risks which can be categorised as:

- Content - sexual, racist, violent unreliable/bigoted i.e. safety of the mind of the child
- Commerce - scams, phishing and pharming, bluejacking, downloads which steal
- information - students and parents
- Contact - via interactive technologies – Instant Messaging, chat, multiplayer games
- Culture - bullying, camera phones, blogging, social networking

Ellis Guilford School has a duty of care, both inside and outside, to protect students from these risks. This policy aims to raise awareness of the risks involved when embracing new technologies for Internet Safety, Internet Security, Media Literacy and communications.

The school's e-safety policy will operate in conjunction with a range of other school policies including those for Student Behaviour, Bullying, Curriculum/Teaching & learning, Data Protection and Security, Prevent.

The E-Safety Policy

2.1 E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by the clarity of the policies
- and the rigorous approach to training and education to ensure consistency in its
- application across the school and through school-home links.
- Sound implementation of e-safety policy in both administration and curriculum, including
- secure school network design and use. This entails clear operational systems and quality assurance procedures to ensure the effectiveness of the policies.

2.2 Teaching and learning

2.3 Why Internet use is 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 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 pupils. Particularly in development of research and other transferable skills and promoting independent learning. Internet use will enhance learning Therefore:

- The school Internet access will be designed specifically for student use and will include filtering appropriate to the age of pupils.
- Students will be taught what Internet use is acceptable and what is not and given clear guidance regarding internet use.
- Internet safety lessons will be delivered through ICT lessons
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Teachers will, where appropriate, screen and identify web based sources that promote

2.4 Pupils will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Unauthorised audio, visual and video files will be removed from the network.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff or students discover unsuitable sites, the URL (or website address) and the content must be reported to the systems manager and such sites will be added to the filtered websites database.

3 Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and / or the Managed Service provider dependent on who is responsible for the network solution at the time.
- Staff will be advised on how to access secure school systems outside of school

3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters, scam and spam or emails containing malicious or offensive materials is not permitted.
- The school has a sanction policy applied to students who infringe their internet access privileges.

- Emails will be scanned when sent for keyword content. Email content which is unsuitable will not be sent and a copy of the offending email copied to the systems manager for follow up with the safeguarding lead. A filtered word list is available upon request.

3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number.
- Staff or pupil's personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified unless specific permission has been granted
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. A standard school proforma has been created for this purpose
- Work can only be published with the permission of the pupil and parents.

3.5 Social networking and personal publishing

- School will block/filter access to social networking sites as well any other application identified at a later date that puts pupils at risk.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

3.6 Managing filtering

- The school will work in partnership with the LA, DfES, The Managed Service provider and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Systems Manager using the helpdesk.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Mobile phones and similar technologies

- Mobile phones are not allowed to be used during lessons and it is advised that they are turned off and placed in the pupil's bag.

- We strongly advise against bringing a mobile phone to school
- Any communication with a student in an emergency should go through main reception
- The sending of abusive or inappropriate messages, images, etc. is forbidden and will result in the student being banned from bringing their devices to school.
- The recording of video using a mobile phone during lessons is not allowed

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.
- New and emerging technologies will be researched by the safeguarding lead and the Systems Manager.

3.9 Chromebooks

Chromebooks are regularly used by students at Ellis Guilford School as part of the Chromebook initiative in year 7 as well as other years. More details of the safe use and responsabilities can be found in the Chromebook user agreement/ policy, below is a list of some important details relating to the use of the Chromebooks.

- It is the responsibility of the individual student to keep the Chromebook in good working order.
- Chromebooks will be monitored at home and in school for their internet usage and tracking of websites visited and searches conducted.
- Violation of the acceptable use agreement will be reported to the Chromebook manager.
- Any information contained within the Chromebooks which demonstrates a breach of a UK law will be reported to the police.

3.10 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Only authorised personal will be able to edit personal details stored in the Management Information System
- Whilst it is not possible to prevent loss of data due to mislaying a portable memory device, reminders will be made to staff on the Learning platform and in the staff bulletin Staff will be informed about the consequences of lost data including data files, images and lesson resources.

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read the 'ICT Code of Conduct' before using any school ICT resource. This is published on the school learning platform
- The school will maintain a current record of all staff and pupils who are denied access to school ICT systems.

- Secondary students will be given access to computers with Internet access individually by agreeing to comply with the Responsible Internet Use statement which is issued when they start at the school.

4.2 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 should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The school will ensure that antivirus databases and firewalls are kept up to date. Files copied on the network from CD ROMs, memory stick (or other portable storage device), DVD or laptop will be scanned for harmful content.
- Regular checks are undertaken to ensure illegal content is not stored on the network.

4.3 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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with schools safeguarding procedures (logged on CPOMS).
- Pupils and parents will be informed of the complaints procedure.
- There may be circumstances where police involvement is necessary, in which case the school will establish the legal position early and help to develop a strategy to resolve the issue/s.
- Any complaint made about staff misuse of the Internet must be referred to the business manager who will then refer to the Headteacher should this be necessary

4.4 Consequences for eSafety Infringement

- Depending upon the severity of the first offence the appropriate member of staff (house Team) will discuss the offence and issue a warning to the student. The offence will be logged into the Behaviour Management system (SIMS)
- For serious offences the evidence will be collated and a letter sent home describing the offence committed with associated evidence. This will be accompanied by a telephone call home.
- Students will have their Internet Access terminated for a period of time. This may also prevent the student from accessing files held on the system including examination coursework. All information will be logged into the Behaviour management system.
- Where e-safety has been breached by a student the house team will follow up and apply the school sanction policy where and when appropriate

4.5 Classroom Internet Control

- The school will ensure that staff are trained to use Impero to monitor student activity in the
- classroom, block Internet Access for the whole class or individuals or limit activities to set URL’s

- Impero will be available in all ICT classrooms
- Programming software such as Visual Basic and C++ will be run using a Virtual PC to protect the network from running executable files (.exe)

4.6 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will provide a guest log in username and password for when guest arrive wishing to use ICT facilities. Access to shared drives will only be made if necessary by the systems manager and / or Managed Service provider.
- The school provide a community internet access for students and guests to access the Internet within the school environment using their own devices – laptop PC, Tablet PC or Mobile phone using wireless LAN networking (See Systems Manager for setup)

5 Communications Policy

5.1 Introducing the e-safety policy to pupils

- e-safety rules/advice will be posted in all networked rooms and other classrooms where mobile laptop computers are used.
- Pupils will be informed that network and Internet use will be monitored.
- Sanctions regarding` violation of the eSafety rules within school will be available for parents to read.

5.2 Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff and students will be reminded not to leave work stations logged on. A time period of 5 minutes of inactivity will be set before the Login Window reappears.
- Students and staff (unless permitted) will not be able to download and install executable files from the internet (or elsewhere). Unauthorised files discovered on the network will be recorded and logged by the Systems manager.
- Students found to be accessing banned websites by Proxy (i.e. using a website which allows you to type in the address of a banned website to gain access to it) will be interviewed by the house team and the systems manager.
- For serious abuse cases, a letter will be sent home and the content of the website accessed listed. The website used by the student will be added to the filtered list and passed to the Local Education Authority and / or Managed Service provider
- If inappropriate materials are searched ort accessed through the school's ICT systems, it may be necessary to refer to other agencies including the Police.

5.3 Prevent Duty

- All staff receive additional updates during the annual safeguarding update.
- All internet searches made on school equipment in monitored and any material relating to radicalisation is reported to the house team and the safeguarding lead and an interview is conducted.
- All concerns are reported to the local authority, local police or the counter terrorism hotline.

5.4 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Parents interested in child eSafety matters will be referred to organisations such as CEOP (Child Exploitation and Online protection).
- Advice will be given to parents about filtering systems and responsible Internet use upon request.
- All other communications related issues are documented in the school Communications policy

6 Glossary of Terms

Blog - A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors. MoBlogging is blogging by mobile phone.

Bluetooth - Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.

Bluejacking - Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers.

Caching - The process of temporarily storing files, such as web pages, locally to enable quick access to them in the future without placing demands on network resources.

Chatroom - An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering - A method used to prevent or block users' access to unsuitable material on the internet.

Firewall A network security system used to restrict external and internal traffic.

Hacking - The process of illegally breaking into someone else's computer system, breaching the computer's security.

Information and communications technologies (ICT) - The computing and communications facilities and features that, in an educational context, variously support teachers, learning and a range of activities.

Internet Service Provider (ISP) - A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Personal Digital Assistant (PDA) - A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Pharming - Pharming is similar to phishing, however pharming seeks to obtain information through domain spoofing.

Phishing - An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

Spam - Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing - Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan horses - A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Video Conferencing - The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus - A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam - A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking