Apex Primary School

E-SAFETY POLICY

Reviewed – September 2023 **Next review – September 2024**

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones and personal digital assistants (PDAs)
- Internet communications: email and IM
- Webcams and video conferencing
- Wireless games consoles

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

This E-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

1.0 WHAT ARE THE RISKS

- Receiving inappropriate content
- Radicalisation
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

As e-Safety is a relatively new concept and covers a wider scope than Internet use, a summary of a school's e-safety responsibilities is outlined below. This list will assist in developing a co-ordinated and effective approach to managing e-safety issues.

- The school IT Manager is **Gulraze Akhtar** who will oversee and manage the school IT system including security.
- The E-safety Coordinator – **Melanie Hodgson**
- The e-safety Coordinator will seek advice from the LA e-Safety Officer, and where necessary, the Police.
- The E-Safety Coordinator should maintain the E-Safety Policy, manage e-safety training and keep abreast of local and national e-safety awareness campaigns.
- The school will review the policy regularly and revise the policy annually to ensure that it is current and considers any emerging technologies.
- The school will update its filtering systems regularly to ensure that inappropriate websites are blocked.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse will need to be investigated.
- The school will include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.
- All staff must read, understand and implement the Policy.
- The E-Safety Policy will be made available to all staff, governors, parents and visitors through the learning platform and website.

Implementation and Compliance
No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences

2.0 Teaching and learning
Why is Internet use important?
Developing effective practice in Internet use for teaching and learning is essential.
The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
Internet use is part of the statutory curriculum and a necessary tool for learning.
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.1 Evaluating Internet Content
In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience

material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher.

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

1 Local Area Network Security

- Users must act reasonably
- Users must take responsibility for their network use. For all staff, flouting electronic use policy is regarded as a matter for dismissal.
- Workstations should be secured against user mistakes and deliberate actions, e.g. deleting files and folders.
- Servers will be located securely and physical access restricted.
- The server operating system will be secured and kept up to date.
- Virus protection for the whole network will be installed and current.
- Access by wireless devices must be pro-actively managed.

2 Wide Area Network (WAN) security
Firewalls and switches are configured to prevent unauthorised access.

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet should be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

3 Emails

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive an 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.

4 School Website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.
- The head teacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

5 Use of Images

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published.

6 Social Networking

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space.
- They should consider how public the information is and consider using private areas.
- Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers should be advised not to run social network spaces for student use on a personal basis.

3.0 Social networking between staff and pupils in and out of school

In relation to social media (like Facebook, Twitter, snapchat, Myspace, Instagram, Google+ and Flickr), staff must not:

- Exchange accounts with pupils
- Add pupils to their account as "friends" or encourage them to do so
- Enter chat rooms with pupils
- Correspond with pupils using personal email Addresses e.g. Gmail, Hotmail and Yahoo
- Exchange personal mobile phone numbers with pupils
- Take photographs or videos of pupils without parent/guardian consent
- Take photographs or videos of pupils for non-school purposes
- Send or exchange images or videos of school staff, pupils or any aspect of school operations without authorisation or approval
- Download and store inappropriate images or other inappropriate material on teachers laptop/computers (if applicable) outside school hours and off school sites.
- No school devices are to be taken off site by teachers or children

One of the aims of the above is to prevent undue or inappropriate communication between pupils and staff. Anything that may lead to this, and not mentioned above, is also prohibited.

Failure to comply will result in the breach of Safeguarding Policy and will be dealt with accordingly.

Filtering

- SLT/ Teachers will check the school filtering software (Impero) every two weeks to monitor for any breach in the use of internet throughout the school. Any issues that arise will be investigated and actioned accordingly.
- The school will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety Coordinator.
- This task requires both educational and technical experience.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- An annual review will be conducted of the system

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

4.0 Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for pupil access, online GAFE form.

Internet Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

5.0 Use of Personal Mobile Phones for Staff

The school recognises that personal mobile phones have the potential to be used inappropriately. Mobile phones should never be used to take photographs or videos of children Personal mobile phones should not generally be needed or used by staff, except as set out in the guidelines below.

- Mobile phones should not be used in the presence of the children.
- Mobile phones should not be used during lesson times either to make or receive calls.
- Staff should never give their mobile phone number to any pupils. This also includes past pupils under the age of 18 years
- Mobile phones are allowed to be used on trips for communication purposes between staff

Early years
Mobile phones

Personal mobile phones should be either turned off or on silent and not accessed during working hours. Mobile phones can only be used on a designated break and this must be away from the children. Mobile phones should be stored safely in staff bags at all times during working hours.

CCTV

See CCTV policy

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 head teacher, unless it is the head teacher where complaints will be sent to the Chair of Trustees.
- Pupils and parents will be informed of the complaints procedure via the Concerns and Complaints Policy

- Parents and pupils will need to work in partnership with staff to resolve issues.

Awareness of the policy

- Safety rules will be posted around the school.
- Pupils will be informed that network and Internet use will be monitored.
- Safety training will take place regularly to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included as part of the Computing curriculum.
- All staff will have access to the School E-Safety Policy and its application and 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.
- Parents' attention will be drawn to the school's E-Safety Policy on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

Websites Offering Additional Advice and Guidance

BBC Chat Guide http://www.bbc.co.uk/chatguide/
Becta http://www.becta.org.uk/schools/esafety
Childline http://www.childline.org.uk/
Child Exploitation & Online Protection Centre http://www.ceop.gov.uk
Grid Club and the Cyber Cafe http://www.gridclub.com
Internet Watch Foundation http://www.iwf.org.uk/
Internet Safety Zone http://www.internetsafetyzone.com/
Kidsmart http://www.kidsmart.org.uk/
NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209
NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Schools e-Safety Blog http://clusterweb.org.uk?esafetyblog
Schools ICT Security Policy http://www.eiskent.co.uk (broadband link)
Stop Text Bully www.stoptextbully.com
Think U Know website http://www.thinkuknow.co.uk/
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/