Netherleigh and Rossefield School

E-Safety Policy

October 2017

E-Safety Policy - introduction and definitions

The policy should be read in conjunction with the Anti-Bullying Policy, Personal, Social, Health and Economic Education & Citizenship (PSHEEC) Policy and Safeguarding Policy.

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in School and, more importantly in many cases, used outside of School by children include:

- the internet;
- e-mail;
- instant messaging (http://www.msn.com , http://info.aol.co.uk/aim/) often using simple web cams;
- Blogs/Twitter/Snapchat etc. (and other on-line interactive diary/discussion forums etc.);
- podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player);
- social networking sites (Popular www.facebook.com / www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com);
- video broadcasting sites (Popular: http://www.youtube.com/);
- chat rooms (Popular www.teenchat.com , www.habbohotel.co.uk);
- gaming sites (Popular www.neopets.com , http://www.miniclip.com/games/en/ , http://www.runescape.com/);
- music download sites (Popular http://www.apple.com/itunes/ and http://www.apple.com/uk/ios/facetime/ http://www.napster.co.uk/ http://www.kazzaa.com/ , http://www-livewire.com/ https://www.spotify.com)
- mobile phones with camera and video functionality;
- smart phones with e-mail, web functionality and cut down 'office' applications; and
- tablet computers with http://www.apple.com/uk/ios/facetime/ and all the above functions and more.

E-Safety highlights the need to educate pupils and employees about the benefits and risks of using this technology and provides safeguards and awareness for users to enable them to control their online experience.

This Policy establishes the ground rules that the School has for using the internet, electronic communications such as mobile phones, mobile tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using

technology and provides safeguards and awareness for users to enable them to control their online experiences. It also describes how these ideas fit in to the wider context of child protection, exploitation, discipline and PSHEEC policies and demonstrates the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Previously the School's approach to E-Safety was incorporated within other policies. This is now a stand alone policy and renamed as the School's E-Safety Policy. This reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. Employees have signed to confirm that they have read the whole School approach to Computing contained in the Staff Acceptable ICT Use Policy.

The School's E-Safety Policy should operate in conjunction with other policies including: Safeguarding, Anti-Bullying, Curriculum, SMSC and School rules and the Mobile Phone Policy.

Roles and responsibilities

Safety is recognised as an essential aspect of strategic leadership in the School and the Head, with the support of the Proprietors, aims to embed safe practices into the culture of the School. The Head ensures that the Policy is implemented, and compliance with the Policy monitored. The responsibility for E-Safety has been designated to the Computing Coordinator.

It is every teacher's responsibility to be aware of cyber-bullying and its results. The following short video should be viewed by employees and this will be shown in PSHEEC lessons to Year 5 and 6 pupils.

http://www.digizen.org/resources/cyberbullying/films/uk/lfit-film.aspx

Regular warnings are given to pupils about E-Safety in Computing lessons.

Employees should not leave their laptop/tablet logged in when it is unsupervised.

The name of the School's E-Safety Co-ordinator is Mr Craig Hewitt.

The names of the Designated Safeguarding Leads can be obtained from the Safeguarding Policy.

The E-Safety Coordinator ensures that the School keeps up-to-date with E-Safety issues and guidance through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).

All employees have copies of this policy, and this has been made available to parents on the school website (and upon request at the school office.) E-Safety updates are also referred to in the weekly newsletter.

Whole School E-Safety

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

Responsible computing use by all employees and pupils; encouraged by education and made explicit through published policies.

Sound implementation of E-Safety policy in both administration and curriculum, including secure School network design and use.

Safe and secure broadband, including the effective management of filtering (dual responsibility for this lies with Craig Hewitt: E-Safety Co-ordinator and Richard Maddra: Class Teacher.)

The overriding rule is that no pupil should have any unsupervised access to the computers and tablets within School.

Teaching and 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. Internet use is a part of the statutory curriculum and a necessary tool for employees and pupils.

Internet use that will enhance learning

- The School internet access will be designed expressly for pupil use and will include filtering. **No site should be visited by pupils unless the teacher in charge has first visited the site and checked out links.** Obviously extreme sites are filtered, as are gaming sites but occasionally as with all systems things can creep through. There are, however, several sites used by the School that are child friendly and developed specifically for Schools and these sites are acceptable for pupils to investigate and produce independent research without any worries about E-Safety.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation of information. Indeed, the School should constantly emphasise critical thinking. Critical thinking indicates that the School should not spoon feed children and should encourage them to research and find information for themselves whilst always being critical of what they are learning. This is particularly so in this digital age where anyone can post information on the internet without checking that what they have submitted is correct.

- Teachers will ensure that the use of internet-derived information, for research and projects, complies with copyright law. Pupils should be made aware that the internet is not a free for all and that much of its content is covered by copyright law.

- Pupils should be taught to be critically aware of any internet-derived material that they read and shown how to evaluate and validate the content before accepting its accuracy.

- The School's PSHEEC scheme of work also covers cyber-bullying and its consequences.

Managing internet access

- School computing systems capacity and security will be reviewed regularly.

- Employees' and pupils' use of the internet is monitored. Any unacceptable use will be identified by one of Craig Hewitt or Richard Maddra and discussed with the Headmaster, who will decide on the action to be taken.

- Virus protection and restricted sites are updated regularly.

• When using search engines to access information from a range of websites pupils must always be supervised and the search carried out by the teacher prior to the lesson to avoid any unsuitable names and sites cropping up.

• Tablets are also available in School. It is here that controlled access to the internet is vital. It is inevitable that this Policy will require further updates as tablets become more integrated within lessons.

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. This will be checked to the E-Safety Co-ordinator, who will discuss its content with the Headmaster. The Headmaster will decide on any further action.

• Pupils must be told not to reveal personal details of themselves or others in any e-mail communication, or arrange to meet anyone.

• E-mail sent to an external organisation should be written carefully and authorised by a member of staff before sending, in the same way as a letter written on School headed paper.

• The forwarding of chain letters is not permitted. In reality, much of the above should not be an issue as the teacher is required to monitor emails and they should only be sent after they have been read. The School's policy is that emails should be composed using word document software and, having first been approved by the teacher, they are then pasted into an e-mail.

Published content and the School website

• The contact details on the website should be the School address, e-mail and telephone number. Employee names and photographs can be removed if requested.

• All parents are required to sign a form indicating whether or not their child's photograph may or may not be published by the school for promotional purposes (be it online or in print.)

• The School generally avoids the use of pupil names and photographs together on the website except when impossible to do so (an individual sports winner, for example). All parents are asked to opt out should they not want an image of their child to appear on the website.

Employee mobile phone use

- Staff will not carry personal mobile phones while working. Their phones will be kept in an agreed area in the school.
- Staff may use their use their mobile phones during break / lunchtimes in an agreed area not used by children.
- If staff need to make a personal call during a session, they should (with agreement of their line manager), make this in the agreed area not used by children.
- Staff must give the school telephone number to their next of kin, in case it is necessary for the staff member to be contacted, in an emergency during session hours.
- A mobile phone will be taken on all school trips. This is in line with the Statutory framework for the Early Years Foundation Stage which states that providers should take contact telephone numbers and a mobile phone on outings.

Social networking and personal publishing

- The School 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 or their location.
- Pupils and parents will be advised that the use of social network spaces outside School is inappropriate for primary aged pupils.

Managing filtering

If employees or pupils discover an unsuitable site, it must be reported to the Computing teacher/Class teacher, Headmaster or Deputy Head as soon as possible (they will then arrange for the site to be blocked).

Managing video-conferencing

IP video-conferencing should only be used when pupils are with a teacher and permission of the Headmaster has been sought. Video-conferencing will be appropriately supervised for the pupils' age.

Mobile phone use and managing emerging technologies

The following policy will be available in every classroom and each member of staff will be responsible for ensuring that this is implemented.

- New and emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Mobile phones MUST NOT be used by pupils on School premises.
- The taking of pictures and video using a mobile phone is not allowed on School premises.
- The sending of abusive or inappropriate electronic messages, photographs or any other information meant to hurt, tease or cause distress of any sort is forbidden. Pupils should remember that ALL electronic data is recoverable and anything once done cannot be undone. So a picture message or email, once sent, can easily be traced, even once it has been deleted. Class teachers must then inform the Head or Deputy Head, who will decide on any action that needs to be taken.
- Using a mobile phone or email to tease, bully or otherwise upset pupils, even if outside School, may be punishable within School.
- Pupils must note that there is no difference between name calling etc. by mobile phone, text or email and verbally teasing someone and it will be treated the same way.
- No pupil should bring into School any form of electronic game, iPod, or similar MP3 players.

Protecting personal data

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

Handling E-Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of employees. Pupils can, in accordance with the Anti-Bullying, Safeguarding and other policies, approach any member of staff with a concern.

- Any complaint about employees misuse must be referred to the Headmaster.

- Complaints of a child protection nature must be dealt with in accordance with the School Safeguarding Policy.

The School will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a School computer or mobile device. The School cannot accept liability for material accessed, or any consequences of internet access.

Employees and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by E-Safety Coordinator/Headmaster;

- informing parents or carers;

- removal of internet or computer access for a period, (which could ultimately prevent access to files held on the system);

- referral to the Designated Safeguarding Lead and, in extreme situations, the police.

Introducing the E-Safety policy to pupils

- E-Safety rules will be discussed with the pupils at the start of each year in their Computing lessons.

- Pupils are informed that network and internet use is monitored.

- Lessons on E-Safety will now form part of the Computing curriculum. Details of this can be seen in the computing document and the schemes of work for each year group.

- Each year, Years 4, 5 and 6 will have PSHE lessons which focuses on E-Safety and cyber bullying, including discussions about this topic.

- A mobile phone policy will be available in each classroom.

Employees and the E-Safety policy

- All employees will be given this School E-Safety Policy and its importance explained.

- Up to date E-Safety training will be undertaken. For September 2016 all employees will have had training on online safety, social media, its effects and consequences.

- Employees should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Photographic and video images (Taken from Code of Conduct)

It is good practice at times to record photographic and video images of pupils, or to allow pupils to record images of each other to assist teaching and learning, or to celebrate achievement. There is, however, potential for images of children to be misused, in extreme

cases for pornographic or grooming purposes. Employees should therefore adhere to the following code:

- only record images when there is a justifiable need;
- ensure that pupils understand the reason for the recording of the images and how the images will be used and stored;
- ensure that a senior colleague is aware of the recordings;
- ensure that all images recorded are available for scrutiny;
- avoid making recordings in one-to-one situations;
- on admission to the School, parents give consent that images and recordings of their children can be used for legitimate reasons;
- if a photograph is used, the pupils should not be named without direct parental consent; and
- where the School has decided that images should be retained for future use, they should be stored and used only by those authorised to do so.

Internet use

- Employees must follow the School policy on the use of ICT equipment and the internet. Accessing child pornography, or making, storing or disseminating such materials is illegal and, if proven, will be treated as gross misconduct and may lead to dismissal. Employees must not use School ICT equipment to access adult pornography on or off site.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the School website. A document giving advice to parents about safe internet use at home will be sent to parents.

- Pupils and parents are informed of the Exploitation and Online Protection Centre: www.thinkyouknow.co.uk.