Chair of Governors: Mrs T Hussain
Acting Head Teacher: Mr Carter

Online Safety Policy

Current Policy Date: Autumn term 2016
Review: Annually
Date of Next Review: Autumn term 2017

Online Safety encompasses Internet technologies and electronic communications such as mobile phones as well as 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 experience.

Online Safety depends on effective practice at a number of levels:

- Responsible COMPUTING use by all staff and students
- Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from LA-ICT including the effective management of Net sweeper filtering *and Policy Central software.*
- National Education Network standards and specifications.

Online Safety Curriculum coverage

KS1 targets overview:

Knowledge and understanding
•Can they understand the different methods of communication (e.g. email, online forums etc)?

•Do they know you should only open email from a known source?
•Do they know the difference between email and communication systems such as blogs and wikis?
•Do they know that websites sometimes include pop-ups that take them away from the main site?
•Do they know that bookmarking is a way to find safe sites again quickly?
•Can they begin to evaluate websites and know that everything on the internet is not true?
•Do they know that it is not always possible and legal to copy some text and Computing pictures from the internet?
•Do they know that personal information (name, age, gender) should not be shared online?
•Do they know they must tell a trusted adult immediately if anyone tries to meet them via the internet?

Skills
•Can they follow the school's safer internet rules?
•Can they use the search engines agreed by the school?
•Can they act if they find something inappropriate on line or something they are unsure of (including identifying people who can help; minimising screen; online reporting using school system etc)?
•Can they use the internet for learning and communicating with others, making choices when navigating through sites?
•Can they send and receive email as a class?
•Can they recognise advertising on websites and learn to ignore it?
•Can they use a password to access the secure network?

KS2 targets overview:

Knowledge and understanding
•Can they discuss the positive and negative impact of the use of COMPUTING in their own lives and those of their peers and family?
•Do they understand the potential risk of providing personal information (name, age, gender) online?
•Do they recognise why people may publish content that is not accurate and understand the need to be critical evaluators of content?
•Do they understand that some websites and/or pop-ups have commercial interests that may affect the way the information is presented?
•Do they recognise the potential risks of using internet communication tools and understand how to minimise those risks (including scams and phishing)?
•Do they understand that some material on the internet is copyrighted and may not be copied or downloaded?
•Do they understand that some messages may be malicious and know how to deal with this?
•Do they understand that online environments have security settings, which can be altered, to protect the user?
•Do they understand the benefits of developing a 'nickname' for online use?
•Do they understand that some malicious adults may use various techniques to make contact and elicit personal information?
•Do they know that it is unsafe to arrange to meet unknown people online?
•Do they know how to report any suspicions?

•Do they understand they should not publish other people's pComputing ures, audio, videos or tag them on the internet without permission?
•Do they know that content put online is extremely difficult to remove?
•Do they know what to do if they discover something malicious or inappropriate?

Skills
•Do they follow the school's safer internet rules?
•Can they make safe choices about use of technology?
•Do they use technology in ways which minimises risk, e.g. responsible use of online discussions, etc?
•Can they create strong passwords and manage them so that they remain strong?
•Can they independently, and with regard for e-safety, select and use appropriate communication tools to solve problems by collaborating and communicating with others within and beyond school?
•Can they competently use the internet as a search tool?
•Can they reference information sources?
•Can they use appropriate strategies for finding, critically evaluating, validating and verifying information, e.g. using different keywords, skim reading to check relevance of information, cross checking with different websites or other non COMPUTING resources?
•Can they use knowledge of the meaning of different domain names and common website extensions (e.g. .co.uk; .com; .ac; .sch; .org; .gov; .net) to support validation of information?

School Online Safety policy

- The Online Safety Policy is part of the School Development Plan and relates to other policies including those for COMPUTING, bullying and for child protection.
- The school has appointed a named person to co-ordinate e-Safety.
- Our Online Safety Policy has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy is reviewed annually by the ECM Committee.

Teaching and learning

Why Internet use is important

- The Internet is an essential element 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.

Internet use will enhance learning

The school Internet access is designed for pupil use and includes 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.*
- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation*
- *The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.*
- *Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.*

Managing Internet Access

- *Information system security School COMPUTING systems capacity and security will be reviewed annually.*
- *Virus protection will be updated annually.*
- *Security strategies will be discussed with Walsall Local Authority and LA-COMPUTING .*

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.*

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 pupils' personal information will not be published.

- *The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.*

Publishing pupil's images and work

- *Photographs 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 school website particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school Learning Platform.*
- *Pupil's work can only be published with the permission of the pupil and parents.*

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.

Twitter Appropriate Usage Policy

1. The school Twitter account is a broadcast only account and is not intended to be used for the purpose of extended communication.
2. All tweet requests will be submitted through senior management.
3. Staff assume responsibility for communicating with a public audience and representing the school when submitting tweet requests to SMT.
4. Ultimate responsibility for the content of any tweet lies with the administrator publishing the tweet.
5. Administrators may deny a tweet request and will provide prompt written or verbal reasoning to the member of staff requesting the tweet.
6. Content of tweets must always relate to PHP or events that PHP are participating in.
7. Photos and/or links submitted to accompany tweets must be in accordance with PHP publishing guidelines (see above).
8. Tweets naming pupils may only be published with the express written or verbal permission of the pupil concerned, and that of a parent/guardian (established and agreed at the beginning of the year in the home-school agreement pack). Only first names will be used when referencing children.
9. Administrators will block any users bringing the school into perceived disrepute by comments made regarding @PoolHayesP tweets. Justification for such action will only be provided outside of exceptional circumstances.
10. Staff will not use Twitter's private messaging facility to communicate with current or ex school pupils under any circumstances.
11. The school twitter account will not post photos of children's faces; it will post photos of work, learning and school events/notices.

Managing filtering

- The school will work with the Education Walsall, DCFS 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 named Online Safety Coordinator (Miss Guy).
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Mobile phones should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden
- Video conferencing will be appropriately supervised for the pupils' age.
- Emerging technologies will be examined for educational benefit and added to a prevision form risk assessment will be carried out before use in school is allowed.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

PREVENT

Extremism:

The offline risks of terrorism and violent extremism are well-known, and these are mirrored online. Terrorists and violent extremists exploit the internet for both operational purposes and as a tool for radicalisation and recruitment. This represents a serious risk to vulnerable individuals using the internet.

Materials likely to be useful in preparing, instigating or conducting an act of terrorism. This would include, for example, bomb-making instructions, explosives manuals, explanations of how to manufacture poisons and weaponry, and targeting information.

Ideological materials inciting violence and/ or hatred. This could include videos of fatal attacks against soldiers or beheadings with accompanying messages of glorification. Speeches and essays by individuals advocating racial or religious supremacy, actively stirring up hatred against other groups would also fall into this category, as would chat forums containing postings encouraging others to emulate the activities of terrorists or bigots.

It is recommended that parents and those with responsibility for vulnerable individuals follow standard guidance on online safety, such as that provided by ParentCentre (http://www.parentscentre. gov.uk/usingcomputersandtheinternet/) and The Child Exploitation and Online Protection Centre (www. thinkuknow.co.uk).

COMPUTING access

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff must read and sign the 'Acceptable Use Agreement' before using any school COMPUTING resource (unless completed electronically through 'Policy Central' or CC4).
- The school will keep an up to date record of all staff and pupils who are granted Internet access.
- Pupils' access to the Internet will be under adult supervision at all times.
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user
- Online Safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school Web site.
- Parents will be asked to sign and return an Internet access/publishing consent form, manually or when necessary.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Education Walsall can accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with by the Head Teacher.
- SMT/COMPUTING Leader will undertake an Online Safety audit each year (See Online Safety audit document in the leadership file) to assess whether the Online Safety basics are in place.

Note. To be ratified March 2017