WHITEHALL PRIMARY SCHOOL E-SAFETY POLICY

Introduction

E-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.
The E-Safety Policy relates to other policies including those for Computing Curriculum, Behaviour, Safeguarding and Child Protection.

The Head Teacher will act as the E-Safety Coordinator in conjunction with being the Designated Child Protection Coordinator (DSP) as the roles overlap.

Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by the School Leadership Team and approved by the Governors.

Teaching and Learning

Why Internet and Digital communication are important

- The Internet is an essential element in 21st century life for education, business and social interaction. Whitehall 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 staff and pupils.

Internet use will enhance learning

- The school Internet access is designed expressly for pupils use and will include filtering appropriate to the age of the 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.
- Pupils will be shown to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant and inappropriate Internet content.

Managing Internet Access

Information system security

- The schools security filtering levels (managed by RM) are checked regularly by the Network Manager.
- Virus protection will be updated regularly.

E-mail

- Staff and pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- 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 is not permitted.

Published content and the school website

- The contact details on the school website should be the school address, e-mail and telephone. 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

- All digital photography will be taken using school devices. No photos/videos will be taken on personal devices.
- Photographs that include pupils will be selected carefully so that pupils cannot be identified or their image misused.
- Pupil's 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 website.
- Photographs used for assessment purposes in the Early Years will be stored on a separate secure server. Parental permission will be obtained before photographs are taken.
- Pupil's work will 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 that 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.
- Staff must be aware of the potential risks regarding the use of social networking sites and post content (comments and photographs) appropriately.

Managing Filtering

- The schools broadband and internet filtering is provided by RM and has a minimum IWF level filtering policy. The internet filtering can be adjusted to suit staff requirements and age appropriate use for students if required. Adjusted levels of internet use require a secure password and all internet access is recorded by the provider and can be reviewed if necessary.

- If staff or pupils come across unsuitable on-line materials, the site must be recorded on an incident form and reported to the E-Safety Coordinator. This will then be reviewed by the SLT and appropriate action will be taken and recorded.

Managing Videoconferencing

- When this becomes available within school, videoconferencing will only be used within the internal school network. In future, we may be able to video link with other schools.
- Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and web cam use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- The School Leadership Team must note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Protecting personal data

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

Policy Decisions

Authorising Internet Access

- All staff must read and sign the Acceptable Use Policy (AUP) before using any school ICT resource (Appendix 1)
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return an Acceptable Use Policy for their child. (Appendices 2,3,& 4)
- Any persons not directly employed by the school i.e. supply staff have a restricted access login and a restricted access to SIMS to complete registration.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor the Local Authority can accept liability for any material accessed, or any consequences of Internet access.

- 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 and effective

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the School Leadership Team.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature will be dealt with in accordance with the school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications policy

Introducing the E-Safety Policy to pupils

- E-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-safety training will be embedded within the Computing Curriculum also linking to the PSHCE curriculum.

Staff and the E-Safety Policy

- All staff will have access to the school E-Safety Policy and its importance explained.
- Staff must be informed that network and the Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters, the school prospectus and on the school website.

Nayna Gareja
Computing Curriculum Leader
September 2015

Approved by the Governors on:

Review Date: September 2018

APPENDIX 1

Whitehall Primary School
Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, hand held devices, digital cameras, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the System Manager (Paul Ellam).
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site should only be on school provided equipment (laptops or memory sticks). Any images or videos of pupils will only be used in the school image and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information
(including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). I will protect the devices in my care from unapproved access or theft.
- I will not connect personal devices (including laptops, mobile phones, iPods, etc) to the school network without prior authorisation from the Head Teacher.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.

- I have read and understood the school E-Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety on an Incident form and hand it to the Designated Child Protection Coordinator (Head Teacher - Anna Boychuk) as soon as possible.
- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Nayna Gareja) the Computing Curriculum Leader or (Paul Ellam) the designated lead for filtering as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Technical Manager (Paul Ellam) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the School Leadership Team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence,
inconvenience or needless anxiety to any other person, or anything which could bring my professional role,
the school or the City Council into disrepute.
- I will promote E-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Head Teacher or the ICT Technical Manager.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……..... Print Name: ...……. Date: …….....

APPENDIX 2

Whitehall Primary School Acceptable Use Policy (AUP)

Early Years Foundation Stage

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.

	I will use school computers for school work and not to upset or be rude to other people. I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly. I will log off or shut down a computer when I have finished using it.
	I will save only school work on the school computer and will check with my teacher before printing.
	I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.
	I will only go on websites that my teacher tells me to. I will tell my teacher straight away if I go on a website by mistake. I will tell a teacher straight away if I see a website that is not my work.

I will read and follow these rules.

I understand that all of my work on school ICT equipment can be seen.

I understand that I must follow these rules or I will be in trouble.

Parent/Carer's Signature:…… Date:……

Parent/Carer's Name:……

Child's name: ……

Class:……

APPENDIX 3

Whitehall Primary School Acceptable Use Policy (AUP)

Key Stage 1

I will read and follow the rules in the AUP.
I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it.

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.
- I will use school computers for school work and not to upset or be rude to other people.
- I will only use my school email account (which ends .sch.uk) in school.
- I will not open any email attachments without checking with an adult.
- I will only go on websites that my teacher tells me to.
- I will tell my teacher straight away if I go on a website by mistake.
- I will tell a teacher straight away if I see a website that is not my work or receive emails from people I don't know.
- I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly.
- I will not try to download or install any software on school computers.
- I will only use the username and password I have been given and I will keep them secret.

- I will save only school work on the school network and will check with my teacher before printing.
- I will log off or shut down a computer when I have finished using it.

I understand that all of my work and internet activity on school ICT equipment can be seen

I understand that I must follow these rules or I will be in trouble

Parent/Carer's Signature:…… Date:……

Parent/Carer's Name:……

Child's name: ……

Child's Signature:……

Class:……

APPENDIX 4

Whitehall Primary School Acceptable Use Policy (AUP)

Key Stage 2

I will read and follow the rules in the AUP.
I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it.

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy

- I will only use school ICT equipment for my school work and not to upset or bully other people or create a bad impression of my school.
- I will take responsibility for my own use of all ICT equipment and will use it safely, responsibly and legally e.g.
- I will only use my school email account (which ends .sch.uk) in school.
- I will not open any email attachments without checking with an adult.
- I will make sure that my work does not break copyright.
- I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake I will tell a teacher straight away.
- I will tell a teacher if I can see a website that is inappropriate or receive any unwanted emails (such as spam).
- I will look after school ICT equipment and report any damage to a teacher straight away.
- I will not try to get past any security measures in place to protect the school network.
- I will only use the usernames and passwords I have been given and I will keep them secret (including embc and/or Fronter usernames and passwords).

- If I have to use a flash drive (USB memory stick) in school I will ask for permission from the teacher and I will run an anti-virus check on it before I open my files.
- I will save only school work on the school network and will check with my teacher before printing.
- I will log off or shut down a computer when I have finished using it.

I understand that all of my work and internet activity on school ICT equipment can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly.

Parent/Carer's Signature:……. Date:……

Parent/Carer's Name:…….

Child's name: ……

Child's Signature:…….

Class:…….