Whitehall Infant School

e-Safety Policy
(Updated 2014)

Philosophy

The internet is a powerful learning tool and plays a key role in communication and learning within contemporary society. It is our responsibility to provide children with the necessary skills and awareness to enable them to access and use the internet in a safe and effective way, both in school and at home.

Aims

- To ensure children are aware that there are dangers in the online world, and teach them how to take precautions against these dangers.
- To establish a basis for appropriate use of online communication tools, enabling children to practice and use these tools in a safe and secure online environment.
- To outline how a secure online Managed Learning Environment (MLE) can be used safely and effectively.
- To provide clear guidelines to teachers and school staff with regards to protecting pupils at Whitehall Infant School.
- To ensure eSafety is embedded and taught consistently across our school.

Acceptable Use of the Internet

All members of the school community will need to agree to an Acceptable User Policy (see Appendix), before they are given access to ICT technology within the school. This forms part of the school's induction procedure for staff, and will need to be completed at the start of each academic year for both staff and pupils. Any breach of the policy should be brought to the attention of the ICT co-ordinator, or the school's Child Protection Officer, if appropriate.

Sanctions for improper use of the ICT could include:

- interview/counselling by Class Teacher / Phase Leader / e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period;
- referral to LA / Police.

For incidents of cyberbullying, please also refer to the school's anti-bullying policy.

How eSafety is taught at Whitehall Infant School

Internet use is an essential element of 21st Century learning. The school has a duty to provide quality internet access for their pupils. The purpose of internet use in school and through the ESchools Learning Platform at home is to raise educational standards, to promote pupils achievement, to support the professional work of staff and to enhance the school's management functions.

Pupils use the internet widely outside school and need to learn how to use it and evaluate internet information and take care of their own safety and security.

Good planning and preparation is critical in ensuring a safe starting point for the development of web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

Equal Opportunities

It is important to value, build upon and benefit from, the cultural and linguistic experiences that children bring with them to the classroom.
Positive images shall be promoted at all times in relation to race, gender, language and ability. (Refer also to the Equal Opportunities Policy.)

Special Needs

Additional planning shall be carried out to ensure that children with special needs are given the opportunity to use the internet and online material in a safe and effective way. This will apply to those who need additional support and to the more able pupils who need extra stimulation and challenges. Provision shall also be made available for those with physical and mental disabilities. (Refer also to the Special Needs Policy.)

Accessing the Internet in School

Our school network is managed by Hillingdon Grid for Learning, and consequently, there are filters in place which prevent access to many sites which may contain inappropriate material. These filters are not always able to block all content and staff should take precautions when accessing the internet with children.

- Internet access should be planned to enrich and extend learning activities. Staff will select sites which support learning outcomes and are appropriate for pupils' age and maturity.
- It is important that staff check that all of the information on a webpage being viewed is appropriate.
- Pupils will be encouraged to tell an adult immediately if they encounter any material that makes them feel uncomfortable. All computers contain the 'Hector Safety Button' which pupils are taught to use to block the screen when they see something they do not like.

eSafety on the MLE

At Whitehall Infant School, we use the London MLE (powered by Fronter). This is a secure online learning environment which can be used to provide opportunities for learning outside of the school environment. As a school, there are measures we need to take to ensure our pupils can use the MLE safely:

- The MLE is a secure site. Only members of our school community are able to access the site and view information and pictures. Children are taught to keep their passwords a secret in order to protect their virtual school.
- When publishing information on the MLE, all material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name. Teachers may use the MLE to share photographs of what children are doing at school. These photographs should never be named. Photographs will preferably be taken as group shots. Parental consent must be obtained at the start of the school year before any photographs are published on the MLE (see guidelines for use of digital images – Appendix)
- Teachers should always check that any page linked to contains only material appropriate for your child to see. Teachers cannot be expected to check all secondary links, but should take reasonable care to ensure that the children cannot easily access inappropriate material. If any inappropriate secondary links are identified, the primary link should be removed from the MLE immediately.
- Children use the computers in school in an environment where they can be monitored effectively.
- The settings on the MLE have been adapted to ensure that children are not allowed to edit their own personal details, or view the personal details of other users within the MLE.
- There is an eSafety room on the MLE, which provides information to parents and children regarding internet safety.

Managing Systems

The security of the school information systems will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies will be discussed with appropriate advisers.

- Personal data sent over the Internet will be encrypted or otherwise secured.

- Portable media may not 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 e-mail.

- Files held on the school's network will be regularly checked.

- The ICT leader / network manager will review system capacity regularly.

Email Monitoring

E-mail is an essential means of communication for both staff. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created. Strategies to support E-safety:

- Access in school to external personal e-mail accounts will be blocked.
- Social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations 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.
- Staff emails are monitored and logs kept.

Website Monitoring and Safety

Our website celebrate pupils‘ work and promotes the school ethos. The school shares information with other educational professionals.

The website is managed and monitored by a nominated website manager.

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.

Social Networking

- The schools will block/filter access to social networking sites.
- 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 (Instant Messenger) 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.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.

- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others can see the comments.

Web Filtering

- The school will work with HGFL to ensure that systems to protect pupils are regularly reviewed.

- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Leader and in turn to HGFL.

- The ICT Leader and the Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (appendix 1).

- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by HGFL.

- The Network Manager will report any virus issues to HGFL.

Video Conferencing

Video conferencing sessions at Whitehall are always led by a trained teacher. They ensure the session is planned, appropriate and understand safety aspects.

- The equipment must be secure and if necessary locked away when not in use.

- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

- Teachers should report any issues to the ICT Leader.

Safeguarding Children Online

The school needs to help pupils to understand internet security through:

- Using safe online training websites
- Discussing safety issues and modelling safe internet use.
- Reporting concerns immediately

- Providing access to only appropriate web filtering and email monitoring systems

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.

Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully

- Processed for specified purposes

- Adequate, relevant and not excessive

- Accurate and up-to-date

- Held no longer than is necessary

- Processed in line with individuals rights

- Kept secure

- Transferred only to other countries with suitable security measures.

Appropriate Usage Policies

All staff, parents, pupils and Governors have to read and sign a code of conduct when issued with their USO Login and Password.

Staff and pupils also read and sign a code of conduct for internet use and email use.

Pupils Permission to use the Internet

- Each year parents read and sign an internet use code of conduct for their child.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

- All staff must read and sign the e-safety Code of Conduct before using any school ICT resource and sign an appropriate use policy

- Parents will be asked to sign and return a consent form for pupil access.

- Parents will be informed that pupils will be provided with supervised Internet access.

Risk Assessment

- 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. Neither the school nor HGFL can accept liability for the material accessed, or any consequences resulting from Internet use.

- 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 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.

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.

- Pupils and parents will be informed of the complaints procedure.

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

- Sanctions within the school discipline policy include:

- Interview/counselling by the member of the senior management team

- Informing parents or carers;

- Removal of Internet or computer access for a period.

Publication of e-safety policy

- E-Safety rules will be posted in key ICT areas

- Pupils will be informed that network and Internet use will be monitored.

- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

- Instruction in responsible and safe use should precede Internet access.

- All staff will be given 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.

- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

Parental Engagement

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, on the school website and the MLE.

- E-Safety resources linked on website for parents to access.

- Parents sign internet agreements and appropriate usage policies.

- Internet issues will be handled sensitively, and parents will be advised accordingly.

- A partnership approach with parents will be encouraged. This could include, if necessary, parent evenings with demonstrations and suggestions for safe home Internet use.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

- Parents are updated on contact information on a regular basis

Appendix

Contacts

e-Safety Contacts and References

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

Stop Text Bully www.stoptextbully.com

Think U Know website http://www.thinkuknow.co.uk/

Responsibility for eSafety lies with the ICT co-ordinator and the school's Designated Safeguarding Lead, where appropriate.

This policy should be implemented alongside the school's Safeguarding Policies.