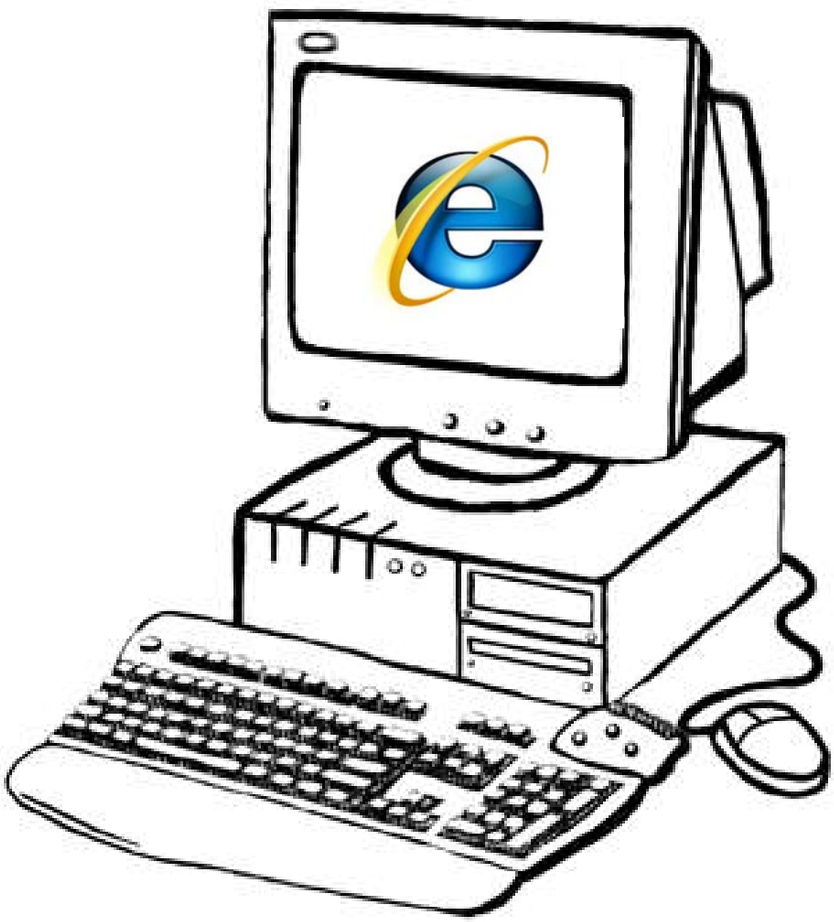
Wormholt Park Primary School



E-Safety Policy

Contents

Wormholt Park Primary School E-Safety Policy

"...the use of information and communication technologies in schools brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications." (Kent Grid for Learning)

1) Who will write and review the policy?

This document forms part of the ICT and Safeguarding Policies. It will also relate to the policies for behaviour, anti-bullying and personal, social and health education (PSHE). It was written in Spring 2011 and will be reviewed on a yearly basis in conjunction with staff. It will be presented to the governing body for approval.

This policy is also in line with our commitment to the UNCRC, in particular article 17: "Children have the right to reliable information from the mass media. Television, radio and newspapers should provide information that children can understand and should not promote materials that could harm children"

The ICT Co-ordinator and designated teacher for Child Protection will oversee E-safety.

2) Teaching and learning

a) Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning. It is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

b) How does Internet use benefit education?

It provides:

- Access to worldwide educational resources including museums and art galleries
- Inclusion in Education Networks which connects UK schools
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Improved access to technical support including remote management of networks and automatic system updates
- Access to learning wherever and whenever convenient.

It promotes:

- Collaboration across networks of schools, support services and professional associations
- Educational and cultural exchanges between pupils worldwide

c) How can Internet use enhance learning?

- Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. These rules will be displayed in classrooms and the ICT suite where there is Internet access.

- 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 will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online 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.

d) How will pupils learn how to evaluate Internet content?

- The quality of information received via radio, newspaper and telephone is variable and pupils needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.
- Pupils in upper KS2 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject.

3 Managing Information Systems

a) How will information systems security be maintained?

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive. Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions. Computers should be 'locked' when appropriate.
- The server is located securely and physical access restricted.
- The servers operating system is secure and kept up to date.
- Virus protection for the whole network is installed and current, with automatic daily updates.
- Technical support for the above is provided by the Kingwood CLC.

Wide Area Network (WAN) security issues include:

- All Internet connections are arranged via the LGFL Schools Broadband team to ensure compliance with the security policy and that firewalls are in place.
- LGFL Schools Broadband Team ensures filtering of content.
- The security of the school information systems and users are reviewed regularly.
- Virus protection is updated regularly and automatically daily.
- Personal data sent over the Internet or taken off site will be encrypted or sent via a secure website.
- Unapproved software 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 coordinator/network manager will review system capacity regularly.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

b) How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools in the local area and in different continents can be created.

There are many implications of email use for the school and pupils, unregulated email can provide routes to pupils that bypass the traditional school boundaries.

Email accounts will not be provided which can be used to identify both a student's full name and the school name. In the majority of cases, whole class or project email addresses are more appropriate.

Pupils

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used in the majority of cases for communication outside of the school.

Staff

- Access in school to social networking sites will be blocked. (have applied for Facebook, My Space, BeBo and Twitter to be blocked)
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper.

c) How will published content be managed?

- Our school website is used to provide contact information, celebrate pupils' work, promote the school and publish resources for projects.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

d) Can pupils' images or work be published?

- Images that include pupils will be selected carefully.
- 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. A permission form is signed when by parents/carers when a child enters the school as part of the Home/School agreement.

e) How will social networking, social media and personal publishing be managed?

- The Internet has online spaces and social networks sites which allow individuals to publish unmediated content. Eg: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.
- Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image, information or comment once published.
- The school will control access to social media and social networking sites.
- Pupils in KS2 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 email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will 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 will be given regarding background detail in a photograph which could identify the student or his/her location.
- Pupils will be advised on security and encouraged to set strong passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils will be advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, racist or homophobic.

f) How can emerging technologies be managed?

- Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for effective and safe practice in the classroom before use in school. .
- We will keep up to date with new technologies, including those relating to mobile phones and handheld devices, and will be ready to develop appropriate strategies.
- The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages will be dealt with under the school's behaviour and anti-bullying policy.

g) How should personal data be protected?

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 school adheres to the following 8 principles of the Data Protection Act of 1998;

Data is:

- 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 individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

4) Policy Decisions

a)How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

b) How will Cyberbullying be managed? (please refer to safeguarding policy also)

- Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007
- Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also being used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
- Cyberbullying (along with all forms of bullying) will not be tolerated in school.
- Children can engage in or be a target of bullying using a range of methods, including text and instant messaging to reach their target. Mobile telephones are also used to capture violent assaults of other children for circulation ('happy slapping'). Children are discouraged from bringing mobile telephones into school. Parent/carers are always advised if a child brings in a mobile telephone. If children do need to bring them, they are given to the School Office and collected at the end of the day.
- Year Six receive a talk from our Community Police Liaison Officer about Cyber-bullying and other issues will be addressed when appropriate or required.
- The school is guided by Hammersmith and Fulham Local Safeguarding Children Board 'E-safety Strategy and Action Plan, 2009-2012'.

5) Communication Policy

a) How will the policy be introduced to pupils?

- Many pupils are very familiar with mobile and Internet use and culture and it is appropriate to involve them in the designing of rules to use when accessing the internet.
- Posters appropriate to each Key Stage will be displayed in classrooms next to classroom computers and in the ICT suite to remind children of the e-Safety rules at the point of use.
- E-safety lessons will be taught as part of the ICT curriculum, either as an ICT lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet. These will be appropriate to the age and will address the importance of safe and responsible internet use both within school and at home.
- Useful e–Safety programmes include:
    - Think U Know: ***www.thinkuknow.co.uk***
    - Childnet: ***www.childnet.com***
    - Kidsmart: ***www.kidsmart.org.uk***

b) How will the policy be discussed with staff?

- The E–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user, discretion and professional conduct is essential.

c) How will parents' support be enlisted?

- Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home
- The Kingwood CLC in conjunction with school, will deliver a parent E-safety awareness session as part of our Service Level Agreement when required.
- There will be advice and help about E-safety issues on our school website.