Greenslade Primary school E safety and acceptable use of the Internet policy for staff, parents and pupils

Why Internet use is important

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is part of everyday life in education, business and for social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.

Use of the Internet for teaching and learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Staff will always use a suitable and safe search engine when accessing the web with 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 how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate Internet content
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content

Managing Internet access

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- The School ICT system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed adjacent to all classroom workstations, in the ICT suite and on the laptop trolley.
- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator/ e safety co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- 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. The school cannot accept liability for any material accessed, or any consequences of Internet access but will take every possible action to limit access to this material.

E mail

- Pupils may only use approved email accounts on the school system. These will be set up by the class teacher and/or ICT co-ordinator, having established all the relevant security and filtering systems are in place.
- Pupils must not reveal their personal details or those of others, or arrange any other type of contact with anyone without permission from an adult.
- Pupils must immediately tell an adult if they receive offensive email.
- Access in school to personal email accounts is blocked (this includes staff)
- The forwarding of chain messages is not permitted

Published content and the school's website

- The school website is a tool for communication and celebration of pupils' achievements.
- Parents and carers will be asked to indicate on forms (admissions and contact details) when photographs of pupils are not to be published on the school website
- Staff and pupil personal details will not be published. The only contact details given online will be those of the school office.
- The website complies with current guidelines for publications including respect for intellectual property rights and copyright.

Social networking and personal publishing

- Primary age pupils are not permitted to use social network sites such as Facebook.
- Access to these sites is prohibited through the LGfL security systems.
- The school will work closely with parents to encourage vigilance at home over children's access to these sites. Other users at home should log out of each session before leaving a computer or tablet unattended for any period.
- Children will be encouraged to think about the ease of uploading personal information to social networks, the associated dangers and the difficulty of removing inappropriate images of information once it has been uploaded.

- Members of staff are not permitted to communicate with pupils online, unless through pre-approved, securely managed sites that are used purely as an education platform (e.g. bookclub blogs, class wiki page). Pupils are not permitted to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory. A named member of staff will take responsibility for monitoring activity on the site and appropriate actions will be taken in the event of protocol breaches (for example the removal of access privileges).
- Members of staff need to be aware of the importance of considering the material they post when away from school, ensuring profiles are secured. They should consider how publishing unsuitable material may affect their professional status; examples include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger.

Filtering systems

- The school works with LGfL to ensure that systems to protect children are reviewed and improved.
- The school's broadband/ wifi access includes filtering appropriate to the age of the pupils.
- If staff or pupils discover an unsuitable site, they must report it immediately to the ICT co-ordinator/e safety coordinator who will take the appropriate action.

Managing emerging technologies

- We recognise that many emerging technologies offer the potential to develop new teaching and learning tools, including mobile communications and internet access, collaboration and multimedia tools. A risk assessment (see appendix) should be carried out for each new technology for effective and safe practice in school.
- Members of staff should be aware that technologies such as mobile phones with wireless internet connection may be able to bypass the school's security systems. Therefore, their use is not permitted during lessons.
- Pupils are not allowed mobile phones except in special circumstances when permission has been granted and they are left in the school office between 9am and 3.30pm.

Personal data

- Personal data will be recorded, processed, transferred and made available securely under the Data Protection Act 1998. It will not be shared with third parties without permission.

Authorising Internet Access

- Normally all pupils at Greenslade Primary school will be granted Internet access, with parental permission which is sought through the admissions process. The school will keep a record of any children for whom Internet Access Permission has not been granted.
- All parents, children and staff will read and sign the Internet access and e-safety agreement upon joining the school (see appendix)

Risk Assessment

- Greenslade will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that access to unsuitable material can never occur on a school computer. Neither can Greenslade school or Greenwich LA accept any responsibility for the material accessed or any consequences resulting from Internet use.
- Internet use, procedures to identify, assess and reduce risks, and this policy will be regularly reviewed

Community

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety through information sent home and workshops.
- The school will be sensitive to Internet related issues experienced by pupils out of school e.g. through social networking sites, and will offer appropriate advice and support.

Cyber bullying

- Cyber bullying is defined as 'the use of information communication technology, particularly mobile phones and the Internet to deliberately hurt or upset someone.' (DCSF 2007)
- Greenslade staff and parents will understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.
- We hold regular workshops for staff, parents and pupils about cyberbullying.

How will the policy be introduced to pupils?

• E-Safety rules will be posted in the ICT suite, and each class will have an e-safety poster relevant for their key stage on display in the classroom.

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

• An e-safety staff meeting will be held to raise the awareness and importance of safe and responsible internet use.

• Specific e-safety lessons will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

How will the policy be discussed with staff?

• All staff will have access to an electronic copy of e-Safety Policy.

• The e-safety policy will be shared with all members of staff in a staff meeting.

• Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

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

How will parents' support be enlisted?

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

• A partnership approach with parents will be encouraged.

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

• Interested parents will be referred to organisations listed in appendix

Policy : May 2014

Review: May 2015

Appendix

e-Safety Contacts and References

BBC Chat Guide

http://www.bbc.co.uk/chatguide/

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

Schools e-Safety Blog

http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy

http://www.eiskent.co.uk (broadband link)

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse

http://www.virtualglobaltaskforce.com/