



Tidemill's E-Safety & Acceptable Use Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. Most young people are enthusiastic Internet users - particularly of interactive services like: Email, Chat and Instant Messaging. However, like many exciting activities, there are risky situations to deal with and hazards to avoid. Essential to providing a safe ICT learning environment are robust policies and procedures, clear roles and responsibilities, a comprehensive e-Safety education programme for pupils, staff and parents and an effective range of technological tools to support E-Safety.

Context

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- o The Internet
- o e-mail
- o Instant messaging (www.msn.com) using simple web cams
- o Blogs (an on-line interactive diary)
- o Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- o Social networking sites (www.facebook.com)
- o Video broadcasting sites (www.youtube.com)
- o Chat Rooms (www.teenchat.com)
- o Gaming Sites (www.neopets.com)
- o Music download sites (www.limewire.com)
- o Mobile phones with camera and video functionality
- o Smart phones with e-mail, web functionality and cut down 'Office' applications.

The New Primary Curriculum states that children should apply their ICT knowledge, skills and understanding confidently and competently in their learning and in everyday contexts and that they become independent and discerning users of technology, recognising opportunities and risks and using strategies to stay safe.

Across all the six areas of learning children learn how to:

1. Find and select information from digital and online sources, making judgments about accuracy and reliability;
2. Create, manipulate and process information using technology to capture and organise data, in order to investigate patterns and trends; explore options using models and simulations; and combine still and moving images, sounds and text to create multimedia products;
3. Collaborate, communicate and share information using connectivity to work with, and present to, people and audiences within and beyond the school;
4. Refine and improve their work, making full use of the nature and pliability of digital information to explore options and improve outcomes.

Policies and Procedures

- The school's e-safety policy will operate in conjunction with other policies including: Behaviour, Anti-Bullying, Teaching and Learning and Data Protection.
- Our e-Safety Policy has been written building on BECTA government guidance (as advised by Lewisham LEA). It has been approved by governors after input from staff and parents.
- The e-Safety Policy and its implementation will be reviewed annually and where necessary in cases of reported misconduct or risks.
- All Tidemill staff and pupils are to sign an Acceptable Use Policy detailing the ways staff, pupils and all network users should use our ICT facilities and reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. The AUP is displayed in all classrooms and on lap-top trolleys.
- E -safety will form a key part of the ICT/PSHE/SEAL Curriculum. Children will be made aware of the dangers and risks of using the internet and mobile technologies throughout the school year. This will include during anti-bullying week, e-safety awareness week and an integral part of ICT lessons.

The next review date is: March 2011

Internet Access

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

- The school Internet access will be designed expressly for pupil use and will use the Synetrix and LGfL filtering system.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will not use the internet without having permission from a member of staff.
- Pupils will not use social networking sites in school and will be educated about their safe usage in their own time.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils are forbidden from downloading games or other programmes from the Internet.
- Downloading programs from the internet will be carried out by the IT technician or IT Leader.
- Public chat-rooms and instant messaging are not allowed and are blocked using the school internet filter.
- Access to peer-to-peer networks is forbidden in school.
- Pupils will be educated in 'Information Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or the intellectual property of others.
- Pupils will be taught how to report unpleasant Internet content.

E-mail

- When available, pupils may only use approved school e-mail accounts on the school Fronter Learning Platform. Pupils are not permitted to use their own personal email accounts on school equipment.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.

- Email 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.
- Staff should never use personal email addresses to communicate with pupils. An official school email address will be provided by the ICT Subject Leader.

Managed Learning Environment

- The MLE is provided for use of Tidemill Primary School staff and pupils only. At present access by any other party is strictly prohibited.
- Pupils should never reveal his/her password to anyone or attempt to access the service using another pupil's login details. Pupils should inform the IT leader if they feel their password has been compromised.
- All staff and pupils possess a username and password as a level of security. The correct levels of privilege are applied to the correct users.
- Activity on the Learning Platform will be monitored to ensure that the content posted by users is valid and does not infringe the intellectual property rights of others.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents.
- Pupil image file names will not refer to the pupil by name.
- Pupil image files should be securely stored on the school network.

Video Conferencing & webcam use

- When available, videoconferencing and webcam use will be appropriately supervised.
- Pupils will be taught the dangers of using webcams outside of school.

Portable Devices

- Mobile phones will not be used during school time. Mobile Phones are not to be used in school; for children who walk home alone then they are to be left at the school office at the beginning of each day. The sending of abusive or inappropriate text messages is forbidden.
- Staff should be aware that technologies such as Ultra Portable Laptops and mobile phones may access the internet by bypassing filtering systems and present a new route to undesirable material and communications.
- Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.
- Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. These may not be used in school.

Protecting personal data

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

Roles and Responsibilities

Our e-safety coordinator is: Richard Graham

(Deputy head & SDP responsible for Child Protection)

Support will be provided by Christian Ellis the ICT co-ordinator and his team.

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance; keeps the Headteacher, senior management and Governors updated as necessary; ensures that any e-safety concerns are reported in the first instance to the e-safety co-ordinator who will investigate the concern and take the appropriate action.

Our governor responsible for e-safety is: Paul Doherty

Our Governors has an understanding of e-Safety issues and strategies at this school; is aware of local and national guidance on e-Safety; is updated at least annually on policy developments.

Our staff have e-safety responsibilities: to be familiar with the policy and to adhere to its' procedures and should be familiar with the schools' Policy in regard to:

- Safe use of e-mail.
- Safe use of Internet.
- Safe use of school network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of pupil information/photographs and use of website.
- eBullying / Cyberbullying procedures.
- Their role in providing e-Safety education for pupils.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will always use a child friendly, safe search engine when accessing the internet with pupils. (E.g. Google Safe Search - default settings)

Staff are reminded / updated about e-Safety matters at least once a year.

Managing Internet Access and Other Technologies

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- All staff and pupils possess individual logons and passwords to the school network with appropriate access rights and privileges.
- Virus protection will be installed on all school computers and updated regularly in light of new viruses and Trojan horses that weaken the schools security.
- Staff must ask permission from the e-safety coordinator before installing software on any school machines.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager, the website can be closed but the computer should not be shut down to allow further investigation.

- The IT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Lewisham LEA can accept liability for the material accessed, or any consequences of Internet access.
- The school will give responsibility to the school technician to monitor the use of internet, email and messaging services.
- 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.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety officer.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (See Child Protection Policy)
- Pupils and parents will be informed of the possible consequences for pupils misusing the Internet.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be given a copy of the acceptable use policy that their child has signed. They will be encouraged and supported to monitor their children's use of technology at home.
- The school will provide regular e-safety sessions for parents.

Glossary

Acceptable Use Policy A policy that a user must agree to abide by in order to gain access to a network or the internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar A graphic identity selected by a user to represent him/herself to the other parties in a **chat-room** or when using **instant messaging**.

Becta The Government's lead partner in the strategic development and delivery of its e-strategy.

Chat-room An area on the internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering A method used to prevent or block users' access to unsuitable material on the internet.

Information Literacy The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant messaging(IM) A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-to-peer (P2P) A peer-to-peer network allows other users to directly access files and folders on each others computer. File sharing networks such as 'Lime Wire' create weaknesses in networks security by allowing outside users access to the schools resources.

Spam Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Video Conferencing The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees - almost as it happens.

Poster to be displayed by all computers & explained to children:



When using the Internet



I will only use the Internet when I have an adult's permission.



I will only click on icons and links when I know they are safe.



I will only send friendly and polite messages.



If I see something I don't like on a screen, I will close it down and tell an adult immediately.



Wet Play

During wet play I will **ONLY** go on the websites listed below:



THINK BEFORE YOU CLICK

KS2 children to read and sign AUP before using school computers. Children to sign names agreeing to APU.

Signatures and APU to be displayed by Class Computers.

Rules of Acceptable Use for Computers

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

- ◆ I will only access the system and Fronter with my own login and password, which I will keep secret. I will let Mr Ellis know if I need to change my password.
- ◆ I will not access other people's files.
- ◆ I will only use the computers for school work and homework.
- ◆ Pupils should not download and use material or copy and paste content which is copyright. (Most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the Internet.)
- ◆ I will not bring in memory sticks or disks from outside school unless I have been given permission.
- ◆ I will ask permission from a member of staff before using the Internet.
- ◆ I will only e-mail people I know or my teacher has approved using Fronter. I will only use my School email account.
- ◆ The messages I send will be polite and responsible.
- ◆ I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- ◆ I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.
- ◆ I understand that the school may check my computer files and may monitor the Internet sites I visit.

All children must sign the AUP before using a school computer

KS1 children to read and sign AUP before using school computers. Children to sign names agreeing to APU at bottom. Book of signatures to be hung next to computers.



When using the *Internet*

THINK BEFORE YOU CLICK



| | |
|--|--|
|  | <p>I will only use the <i>Internet</i> when I have an adult's permission.</p> |
|  | <p>I will only click on icons and links when I know they are safe.</p> |
|  | <p>I will only send friendly and polite messages.</p> |
|  | <p>If I see something I don't like on a screen, I will close it down and tell an adult immediately.</p> |
| <p>Wet Play</p>  | <p>During wet play I will ONLY go on these websites:</p>  |
| <p>I understand how to be safe when using the internet. Name: _____ Class: _____</p> | |