E-Safety Policy
2016-2017

Why do we have an E-Safety Policy?
E-Safety encompasses Internet technologies and electronic communications such as mobile devices and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Practice E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the London Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

Contents

Appendix:
Example of e-safety rules
Example of Letter to parents
Example of Staff systems code of conduct

School e-Safety Policy

Our e-safety Policy has been written by the school, building on the Children and Young Peoples' Directorate and Government guidance. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Barclay Primary School has a duty to provide pupils with quality Internet access
Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- 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;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet & network access.
- All staff must read and sign the 'Systems Code of Conduct' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

● If staff or pupils discover unsuitable sites, the URL (web address), time, content must be reported to the teacher and then the e-safety coordinator or network manager.
● School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
● Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
● Pupils are taught to follow the SMART rules when using the internet and these are embedded to ICT lessons.

Email

● Pupils may only use approved e-mail accounts on the school system.
● Pupils must immediately tell an adult if they receive offensive e-mail.
● The school does not publish personal e-mail addresses of pupils or staff on the school website.
● The school manages accounts effectively with up to date account details of users.
● We will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
● We will reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
● We know that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.
● Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
● Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
● The school never uses email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA system.
● All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
● Access in school to external personal e-mail accounts may be blocked.
● 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.

Social Networking

● The School has blocked access to social networking sites and newsgroups unless a specific use is approved.
● Pupils will be advised never to give out personal details of any kind which may identify them or their location.
● Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
● Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
● Staff should be advised not to accept "friend requests" from students and should set any security settings for social networking sites to "high".

Filtering
The school will work in partnership with the Local Authority, LGFL and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing and filming
● Advice from the ICT Manager should be sought before making or answering a videoconference call.
● Videoconferencing will be appropriately supervised for the pupils' age.
● We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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.

Published Content and the School Web Site

● The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. school@thomasgamuel.waltham.sch.uk Home information or individual e-mail identities will not be published.
● Photographs published on the web do not have full names attached;
● The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
● Uploading of information is restricted to our website authorisers: e.g. Office Manager
● The school web site complies with the school's guidelines for publications;
● Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status; Publishing Pupils' Images and Work
● Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
● 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.
● Photographs of children should not be taken using personal mobile phones or cameras.
● Digital images /video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
● Digital images/ videos stored on the school's mobile devices are deleted before the school at the end of the day.

I.C.T. System Security (also see 'assessing risk' section)
● School ICT systems capacity and security will be reviewed regularly.
● Virus protection is installed and is updated automatically.
● Forensic software is installed across the network to monitor profanity and network abuse.
● Internet filtering provided by Synetrics, blocks content that is deemed to be inappropriate.

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

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 the LA can accept liability for the material accessed, or any consequences of Internet access.

● Forensic software is in place to monitor inappropriate material and misuse of the schools computers outside of this policy.

Monitoring Procedures

● Children are reminded that Forensic Software is in place before they log on to a school computer by the teacher leading the lesson.
● Forensic software will take a screen image of any violation and alert the e-safety co- ordinator.
● The e-safety co-ordinator will be notified of any violations by children and the Headteacher will be notified of any by members of staff.
● Violation will be categorised into levels of profanity and dealt with in accordance with LA guidance. (see below)

Categories of Profanity
● Level 1: A screen shot is taken and marked as a False Positive and no action is taken
● Level 2: A screen shot is taken and user is monitored for a week, user moved to the monitoring level for daily monitoring.
● Level 3: A screen shot is taken and user is questioned by e-safety co-ordinator or class teacher and monitored.
● Level 4: A screen shot is taken and a Daniel Lough (Deputy Head Teacher) is informed, appropriate action taken.
● Level 5: A screen shot is taken and the Head Teacher informed and appropriate action taken. Handling e-safety 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.
● Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
● Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Pupils
● Rules for Internet access will be posted in all networked rooms.
● Children will be informed that Internet use will be monitored.
● Children will sign the e-safety code of conduct once in KS1 and again in KS2.
● In order to ensure that the children are safe in class, mobile phones, personal tables and smart watches with communication abilities are to be submitted to the office at the start of the day and collected at the end.

Staff
● All staff will be given the School e-Safety Policy and its importance explained.
● Staff should be aware that Internet traffic can be monitored and traced to the individual user through Forensic software. Discretion and professional conduct is essential.
● Makes training available annually to staff on the e-safety education program.
● A member of staff has certified e-safety training which is updated biannually.

Parents
● Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
● The school runs a rolling programme of advice, guidance and training for parents, including:
● Information leaflets; in school newsletters; on the school web site;
● demonstrations, practical sessions held at school;
● distribution of 'think u know' for parents materials
● suggestions for safe Internet use at home;
● provision of information about national support sites for parents.

E-safety for pupils with additional needs

There are many variations to school policies, populations and resources available to support e-safety initiatives within schools.

Here are some considerations regarding possible ways to support a generic group of children who may require additional support to move forward in safeguarding themselves.

A fundamental part of teaching e-safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.

● This is a difficult area for some pupils who will usually learn rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers. Schools need to consider whether a scheme or resources are applicable or accessible to all school situations where internet access may be possible.
● As consistency is so important for these pupils, there is a need to establish e-safety rules for school that are similar to those for home. Working with parents and sharing information with them would be relevant to all children, but this group especially.
● There will always be exceptions to rules and if this is the case, then these pupils will need to have additional explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the internet.
● It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of what might happen if... without frightening pupils.

How rules are presented could be vital to help these pupils understand and apply some of the rules they need to learn.

● Visual support is usually important to help most pupils' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e. o Uncomfortable o Smart
o Stranger o Friend
● It might be helpful to ask pupils to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms.
● Visual support can be useful but it is more likely that the pupils will respond to multi-media presentations of the rules such as interactive power-point slides, screensavers, spoken recordings of the main rules or sounds that they can associate with decisions they make while using the internet. The really useful thing about these is the repetition and practice that pupils can have with these which may not be so easy if spoken language were used.
● If visual prompts are used to help remember the rules, the picture or image support needs to give the pupils some improved understanding of what the rule is about. It is quite easy to find attractive pictures that link to other abstract ideas not related to internet use i.e. use of a compass to show "lose track" of a search when a head looking confused is more like what happens.
This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers.
● It can be common for peers to set up scenarios or "accidents" regarding what they look for on the internet and then say it was someone else who has done so. Adults need to plan group interactions carefully when raising awareness of internet safety.
● Some pupils in this group may choose recreational internet activities that are perhaps simpler or aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. All members of staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with internet use

For various reasons, pupils with additional needs may find it difficult to explain or describe events when using the internet

● Some pupils might find it easier to show adults what they did i.e. replay which will obviously have its own issues for staff regarding repeating access.
● Some pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions. Some may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.
● Pupils may need a system or a help sound set up on computers which will help them to get adult attention. If pupils don't recognise that they need help, then adult supervision is the safe way to improve their recognition of this.
www.gridclub.com www.kidsmart.org.uk www.thinkuknow.co.uk www.netsmartz.org www.bizzikid.co.uk

E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.
● The school owns the computer network and can set rules for its use.
● It is a criminal offence to use a computer or network for a purpose not permitted by the school.
● Irresponsible use may result in the loss of network or Internet access.
● Network access must be made via the user's authorised account and password, which must not be given to any other person.
● All network and Internet use must be appropriate to education.
● Copyright and intellectual property rights must be respected.
● Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
● Anonymous messages and chain letters are not permitted.
● Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
● The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
● Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Our School e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: Form: Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored. Signed: Date: Parent's Consent for Web Publication of Work and Photographs I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. Parent's Consent for Internet Access I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: Date: Please print name:

Please complete, sign and return to the school office Staff Information Systems Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e- safety policy for further information and clarification.

● The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
● I understand it is no longer acceptable to use personal mobile phones to photograph or video children, or images of children should not be stored on external hard drives or USB devices that are removed from the school premises.
● I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
● I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
● I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
● I will not install any software or hardware without permission.
● I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
● I will respect copyright and intellectual property rights.
● I will report any incidents of concern regarding children's safety to the school eSafety Coordinator or the Designated Child Protection Coordinator.
● I will ensure that any electronic communications with pupils are compatible with my professional role.
● I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ..... Print: ..... Date: .....
Accepted for school: ..... Print: .....

Glossary of Terms

Acceptable Use Policy (AUP) - a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used.

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

E-safety - deploying and developing safety systems based on modern information and communication technologies (ICT).

False Positive – Within Forensic software when a user accesses a word already contained in a document. i.e. a word contained within a website or document to which the user has no control.

Forensic Software – A software solution that allows Barclay Primary School to monitor and enforce the Acceptable Use Policy across the school network

Monitoring section – a place to monitor users within Forensic software who have not followed the policy.

Social networking - Online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.