Durham Gilesgate Primary School
E-Safety Policy

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones 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 Habits

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 Durham.Net including the effective management of content filtering. This is achieved through the use of Smoothwall software which monitors and tracks any inappropriate content sending email notifications and reports to school leaders so that action can be taken
- National Education Network standards and specifications.

Writing and reviewing the E-safety policy

The school's Computing Co-ordinator and named person for Child Protection will write this policy. It will be shared with the senior Leadership Team and Governing Body. The Computing co-ordinator will act as e-safety coordinator.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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.

Internet use will enhance learning

The school Internet access is 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. 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 taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Co-ordinator.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection is updated regularly. The software currently used is PANDA.

Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

E-mail

The durhamlearning.net email system gives anonymity to pupils through the email address they are given. This means the pupil's full name is not available, nor is the location of their school. This system combines the best of practice in pupil email account names. The service is also filtered.

Pupils may only use these approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail 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.

The forwarding of chain letters is not permitted.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published other than staff names and the names of school Governors.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

At the time of publishing this policy we do not publish children's images or work. Consent to do so is currently under development and it is our intention to do so in the future. When this happens the following will apply:-

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, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The school will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. (Smoothwall reports and monitoring will be used to do this)

Managing videoconferencing

On some occasions we have used videoconferencing or Skype. Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the pupils' age.

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.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation May 2018.

Policy Decisions

Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Any computer connecting to our network must be given a certificate in order to access securely. Only the Headteacher, Computing Co-ordinator or ITSS shared technician can do this with the authorisation of the Headteacher.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor NYCC can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

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 head teacher.

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.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

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

South West grid for Learning materials will be used where appropriate.

Staff and the e-Safety policy

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. Discretion and professional conduct is essential.

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.

Cyberbullying

Cyberbullying is 'the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, to intentionally hurt another individual or group".

We recognise that cyberbullying takes different forms: threats and intimidation, harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images), and manipulation.

We recognise that it can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages, the size of the audience, perceived anonymity, and even the profile of the person doing the bullying and their target.

Cyberbullying is most likely to affect pupils but it can also affect members of school staff and other adults; there are examples of staff being ridiculed, threatened and otherwise abused online by pupils.

Cyberbullying, like all bullying, will be taken very seriously by our school. It is never acceptable, and will be dealt with in line with our Policies for Anti-Bulling and Management of Behaviour.

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We use Hector the Protector to hide any webpage we are not sure about..
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.

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.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Edit this poster for display near computers.

Sample Consent Form

Gaining pupils' and parents' agreement to the Rules for Responsible Internet Use is important but requires management. Some schools do this once each year at the same time as checking the home and emergency contact details. The Rules for Responsible Internet Use should be included with the letter to parents to ensure clarity.

For pupils above the age of 16 and not living at home or for pupils 18 or older, the school should be able to rely on the consent of the pupil alone. Otherwise parent's consent must be obtained. It is also wise to obtain parent's permission to publish pupil's work and to publish pupil's photographs on the school Web site, subject to strict safeguards,

Our School

Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil: ***Form:***

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: ***Date:***

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or 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:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed: ***Date:***

This consent form is based, with permission, on the Internet Policy of the
Irish National Centre for Technology in Education.

This Policy Version:- May 2018.