



C of E Primary School

E-safety Policy **January 2011**

The Green Paper '*Every Child Matters*¹ and the provisions of the *Children Act 2004*², *Working Together to Safeguard Children*³ sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks.

* * *

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of

¹ See The Children Act 2004 [<http://www.opsi.gov.uk/acts/acts2004/20040031.htm>]

² See Every Child Matters website [<http://www.everychildmatters.gov.uk>]

³ Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

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

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / <http://www.hi5.com> / <http://www.facebook.com>)
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, <http://www.miniclip.com/games/en/>, <http://www.runescape.com/> / <http://www.clubpenguin.com>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www.kazaa.com/>, <http://www.livewire.com/>)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

All members of staff will work together to create a safe ICT learning environment.

Teaching and learning- the Internet

- The Internet is an essential element in 21st century 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.
- 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 include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and be given clear objectives for Internet use.
- Children will be directed to Internet sites and monitored while using them.
- Benefits of using the Internet allows access to world-wide educational resources including museums and art galleries.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system.

- 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 by a pupil to an external organisation should be written carefully and authorised by the teacher before sending.

Publishing 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.

Publishing pupil's images

- 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/ Learning Platform.

Managing filtering

- The school will work with the LA, DFE 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 Head Teacher or ICT co-ordinator.
- Half-termly checks need to be made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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. This will be carried out by the ICT co-ordinator, who will feedback to the Headteacher.

Authorising Internet Access

- 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.

Assessing risks

The school will take all reasonable precautions to ensure that users only access 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 SCC can accept liability for the material accessed, or any consequences of Internet access.

Communication Policy

With the introduction of the Learning Platforms, an e-safety education program for pupils, staff and parents is being developed.

Introducing the e-safety policy to pupils:

- E-safety posters will be displayed in all classes.
- Children will learn about the rules connected to the safe use of the Internet through suitable e-safety programs:
www.Thinkuknow.org.uk
www.bbc.co.uk/chatguide - BBC ChatGuide
<http://www.gridclub.com> –Grid Club
- Pupils will be aware that they may not be allowed to use the Internet for a given period if they do not comply with the rules.

Staff and the e-safety policy

- Staff training in safe and responsible Internet use and on the school safety Policy will be provided as required.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Useful sites are:

- www.cybermentors.org.uk
- www.teacher.tv
- www.yhgfl.net/esafeguarding
- www.anti-bullyingalliance.org.uk

Enlisting parents' support

- Parents need to be made aware of the dangers connected with the Internet.
- Through an organised workshop the school may be able to help parents plan appropriate supervised use of the Internet at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet could also be suggested.
- Distribute 'Children, ICT & e-Safety' booklet.

Monitor and Review

This Policy will be monitored and reviewed annually

•