# E-Safety Policy



**The e-safety policy relates to other policies including those for ICT, Counter Cyber Bullying and child protection. Our e-safety policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and ratified by governors. The e-safety policy will be reviewed annually.**

## Context

These aims apply equally to the "virtual world" that young people will encounter whenever they use ICT in its various forms. It is known that ICT can offer new weapons for bullies, via websites or sms texting. It is also known that young people have been exposed to inappropriate content when online.

This policy is drawn up to protect all parties – young people, the staff and the school and aims to provide clear advice and guidance on how to minimise risk and deal with infringements

The "staying safe" outcomes include aims that children and young people are:

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

The school's E Safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Computing, Child Protection/ Safeguarding, Individual Curriculum Policies & Data Protection

## Writing the e-safety policy

- The schools e-Safety Coordinator is Lizzy Hegarty. This may be a Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by Governors.

## Teaching and learning

### Why the Internet and digital communications are important

- 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.

### Internet use will enhance learning

- 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 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

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- 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

## Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

## Published content and the school web site

Staff or pupil personal contact information will not generally 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.

## Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.

- Pupils full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs, first names may be used with permission from the parents if there is a purpose e.g. prize winning.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil.
- Pupil image file names will not refer to the pupil by name.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

## Social networking and personal publishing

The school recognizes that whilst most social media sites do not allow children to join them, many children do have access to these sites. Whilst discouraging membership of these sites the school will take appropriate steps to education children about staying safe on-line.

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites,
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

## Managing filtering

- The school will work to ensure systems to protect pupils are reviewed and improved consistently.
- If staff or pupils come across unsuitable on-line materials, the site 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.

## Managing video conferencing & web cam use

- Video conferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing and web cam use 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.

- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

## Protecting personal data

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

## Policy Decisions

### Authorising Internet access

All staff must read and sign the "Acceptable users agreement" before using any school ICT resource.

- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

### Assessing risks

- 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.
- 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 and 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 (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

- Discussions will be held with the Police School Liaison Officer to establish procedures for handling potentially illegal issues.

## Communications Policy

## Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

### Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

### Enlisting parents' and carers' support

- Parents" and carers" attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

## Reviewing the E-Safety Policy

- The e-Safety Policy was revised by: *Lizzy Hegarty*
- It was approved by the Governors on: … … ………………………….
- The next review date is *Summer Term 2016*

## Appendix 1: Internet use - Possible teaching and learning activities

| Activities | Key e-safety issues | Relevant websites |
|---|---|---|
| Creating web directories to provide easy access to suitable websites. | Parental consent should be sought.<br><br>Pupils should be supervised.<br><br>Pupils should be directed to specific, approved on-line materials. | |
| Using search engines to access information from a range of websites. | Filtering must be active and checked frequently.<br><br>Parental consent should be sought.<br><br>Pupils should be supervised.<br><br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | |
| Exchanging information with other pupils and asking questions of experts via e-mail or blogs. | Pupils should only use approved e-mail accounts or blogs.<br><br>Pupils should never give out personal information.<br><br>Consider using systems that provide online moderation e.g. SuperClubs Plus. | |
| Publishing pupils" work on school and other websites. | Pupils' full names and other personal information should be omitted.<br><br>Pupils' work should only be published on moderated sites and by the school administrator. | |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br><br>Photographs should not enable individual pupils to be identified.<br><br>File names should not refer to the pupil by name.<br><br>Staff must ensure that published | |

| | | |
|---|---|---|
| | images do not breach copyright laws. | |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.<br><br>Access to other social networking sites should be blocked.<br><br>Pupils should never give out personal information. | |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br><br>Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers. | |

## Appendix 2: Useful resources for teachers

BBC Stay Safe

www.bbc.co.uk/cbbc/help/safesurfing

Becta

http://schools.becta.org.uk/index.php?section=is

Chat Danger

www.chatdanger.com/

Child Exploitation and Online Protection Centre

www.ceop.gov.uk/

Childnet

www.childnet-int.org/

Cyber Café

http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen

www.digizen.org/

Kidsmart

www.kidsmart.org.uk

Think U Know

www.thinkuknow.co.uk

Safer Children in the Digital World

www.dfes.gov.uk/byronreview/

BBC Chat Guide

www.bbc.co.uk/chatguide

Childline

www.childline.org.uk

Grid Club and the Cyber Café

www.gridclub.com

NCH – The Children's Charity

www.nch.org.uk/information

NSPCC

www.nspcc.org.uk/html/home/needadvice

Stop Text Bully

www.stoptextbully.com

Virtual Global taskforce – Report Abuse

www.virtualglobaltaskforce.com

## Appendix 3: Useful resources for parents

Care for the family

www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute

www.fosi.org

Internet Watch Foundation

www.iwf.org.uk

Parents Centre

www.parentscentre.gov.uk

Internet Safety Zone

www.internetsafetyzone.com