



PDF Complete
Your complimentary use period has ended.
Thank you for using PDF Complete.

[Click Here to upgrade to Unlimited Pages and Expanded Features](#)

E-Safety Policy

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The school will appoint an e-Safety Coordinator.
- Our e-Safety Policy has been written by the school, building on LA and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.
- The e-Safety Policy was revised by: Emma Green
- It was approved by the Governors on: 17th March 2010
- The next review date is (at least annually): March 2011

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 and the needs of the curriculum.
- Pupils will be taught about acceptable and unacceptable Internet use and given clear objectives for its use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Where and when appropriate, pupils will be shown how to publish and present information to a wider audience.

Identify Internet content

to ensure that the use of Internet derived materials by pupils complies with copyright law.

Pupils should be critically aware of the materials they read and will be shown how to validate information before accepting its accuracy.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils will be taught how to report unpleasant Internet content e.g. using Hector Protector.

Managing Internet Access

Information system security

- Login details must not be shared.
- School ICT systems security will be reviewed regularly.
- Virus and Spyware protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails to external bodies are presented and controlled and these should be checked by staff when sent by pupils.
- The forwarding of chain letters is not permitted.
- Users must not send jokes or other materials that the receiver may find offensive.

Published content and the school web site

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher and SLT will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs will be selected carefully so that images cannot be misused.
- Pupils' full names will not be used anywhere on the school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- 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.

ublishing

- The school will control access to social networking sites, and educate pupils in their safe use.
- 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.
- Users should be advised to place only appropriate photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given, regarding background detail in a photograph, which could identify the student or his / her location. (e.g. house number, street name or school.)
- Should we become aware, the school will address and deal with any bullying that takes place through social networking sites, recording the incident and informing parents of the situation.
- Pupils and staff will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing filtering

- The school will work with Peterborough Local Authority, in liaison with Becta, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
- SLT and the E-safety co-ordinator will work closely with Peterborough Local Authority to ensure that filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

- In the event of videoconferencing, the school will 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 videoconference call.
- Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

- Emerging technologies, in particular software, 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.
- Staff will be issued with a school phone, where contact with pupils is required, or where mobile phones are used to capture photographs of pupils.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Policy Decisions

Authorising Internet access

- All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents are required to sign and return a consent form to confirm their child's access to and use of the internet.

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. Neither the school nor PCC can accept liability for any material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of SLT.
- 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 consequences for pupils misusing the Internet.

Community use of the Internet

- Community users coming into school must adhere to the school's e-safety policy.
- The school will liaise and seek guidance from local and national organisations to establish a common approach to e-safety.

Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms with internet access. Users will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.
- E-Safety awareness will be embedded within all ICT schemes of work and addressed through aspects of the PSHE curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and have its application and importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems must follow clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school E-safety policy will be provided as required.

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 Website.
- The school will recommend a list of e-safety resources for parents/carers and advise them of safeguarding measures through a tailor made leaflet.
- A partnership approach with parents will be encouraged. This will include parent sessions with demonstrations and suggestions for safe home Internet use.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

This policy is to be reviewed: March 2011