

Draft E-Safety Policy

The internet and its importance

The purpose of the 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 of information and business administration systems.

The benefits if the Internet on education

- Allow access to world-wide educational resources including museums and art galleries.
- Inclusion in government initiatives such as DFES ICT in schools.
- Educational and cultural exchanges between pupils world-wide.
- Access to experts in many fields for pupils and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with the LEA and DFES.

The Internet and how it enhances learning

The schools Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and ages of the pupils.

How pupils learn to evaluate Internet content

If staff and pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT team. 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.

E-mail and its management

E-Mail sent to external organization should be written carefully and authorized before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

The School Web Site and its management

Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupil's 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.

Chat rooms and Safety

Pupils will not be allowed access to public or unregulated chat rooms. Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasized.

The authorized use of Internet access

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date. At Key Stage 1 Internet access will be adult demonstrated with occasional directly supervised access to specific, approved on-line materials. Parents will be informed that pupils will be provided with supervised Internet access.

Other devices

e.g. mobile phones, PDA's,

How risks are assessed

In common with other media such as magazines, books and video, some materials available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate materials. 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. The school cannot accept liability for the material accessed, or any consequences on Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the *Computer Misuse Act 1990*.

Methods to identify, assess and minimize risks will be reviewed regularly. The ICT team will ensure that the policy is implemented and compliance with the policy monitored.

The use of Newsgroups and E-mail lists

Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

Management of the filtering system

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Team. The ICT Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any materials that the school believes is illegal must be referred to the Internet Watch Foundation. Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible the filtering strategy will be selected to suit the age and curriculum requirements of the pupils.

Staff consultation

All staff must accept the terms of 'Responsible Internet Use' statement before using the Internet resources in school. All staff should be aware of the schools Internet Policy.

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

How system security is maintained

The school system will be reviewed regularly with regard to security.

Virus protection will be installed updated regularly.

Personal data sent over the Internet will be secure.

Unapproved system utilities and executable files will not be allowed in pupils' work area or attached to e-mails.

Files held on the schools network will be regularly checked.

The ICT Team will ensure that the system has the capacity to take increased traffic caused by Internet use.

Complaints procedure

Responsibility for handling incidents will be delegated to the Senior Leadership Team. Any complaints about staff misuse must be referred to the Head.

Parental Support

Internet access will be handled sensitively to inform parents without undue alarm. Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be available to parents.

Pupils at Christchurch benefit from the positive use and educational potential of ICT technology (ICT policy and Data Security). However, there is potential for misuse and harm. Creating a safe ICT learning environment has a number of important elements:

An infrastructure of whole-site awareness, responsibilities, policies and procedures

Christ Church has appointed an E-Safety committee to set, oversee and monitor the standards and policy for the school's acceptable use of ICT. The committee includes a Governor, members of the SLT and other teaching staff. Parent and pupils are consulted in this process.

The Deputy Head Teacher, who has responsibility for safeguarding has been nominated E-safety coordinator, as central contact point for all e-safety issues.

The E-Safety Policy is linked to the Acceptable Use Policy, Data Security Policy and Anti-Bullying Policy. In order to promote and establish safe and responsible online behaviours, wherever and whenever network users go online both at school and in the home and beyond, an acceptable use policy (AUP) has been developed by the school's E-Safety committee with input from children and parents detailing the ways network users can and cannot use ICT facilities.

An effective range of technological tools

- filtering and content control minimise inappropriate content via the network.
- an accredited internet service provider (ISP) is used
- monitoring systems to keep track of who downloaded what, when they downloaded it, using which computer
- up to date anti virus and anti spam system used
- all users have own username and password
- mobile phones are not allowed to be used on the premises
- **A comprehensive e-safety education programme for everyone in your establishment**

- The curriculum is being developed to ensure that the skills and knowledge pupils need to use technology safely and responsibly and manage the risks are taught discretely and in context. This includes facilitating young people to develop their own protection strategies for when adult supervision and technological protection are not available. (See Internet Policy.)
- An annual e-safety day for all KS1 and KS2 pupils highlights aspects of risk and risk management.
- Staff CPD is the responsibility of the Deputy Head Teacher
- Users know what to do if they find websites or emails that are inappropriate or give offence (tell class teacher who passes on to Deputy Head Teacher to action)
- Log of actions kept by Deputy Head Teacher.

A review process which continually monitors the effectiveness of the above.

The Deputy Head Teacher and E-Safety Team (ICT team) is responsible for overseeing general security, administration and compliance with the agreed E-Safety and Acceptable Use Policy.

Internet use by staff and pupils is monitored, policing the usage of their policy and imposing sanctions for misuse (see Acceptable Use Policy)

The E-Safety Team will regularly monitor and review policies with stakeholders (at least annually), more often where new risks are identified.

The team is responsible for ensuring technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

April 2009