

Schools' E-Safety Policy Summary Version, 2006

(A Template to Help Schools Create Their Own Policy)

Schools' E-Safety Policy

Bracknell Forest LA believes in the educational benefits of curriculum ICT use and seeks to educate young people to become effective, reflective and responsible users. Management that recognises dangers and plans accordingly will help to ensure appropriate, effective and safe pupil use. To help achieve this, each school needs to write and implement its own e-safety policy.

The Policy Template Summary

This template is revised and summarised by Bracknell Forest LA based on the original Kent LA policy document. It will help schools to write their own e-safety policy. This summary is mainly comprised of a range of statements that schools can select from to create their own e-safety policy. Alternatively, a school can write its own statements if these are felt to be more appropriate.

For more supporting material, both general and on each set of statements, sample rules for pupils, letters to parents, web links, etc. please see the **full version** of this document.

An effective e-safety policy must be tailored to the needs of each individual school and the discussions generated during its writing/review are a key part of its communication, understanding and acceptance by those who must implement it.

It is important to maintain a sense of perspective, balancing the benefits that the use of ICT can bring, with the perceived threats to pupil safety.

The headteacher and governors should plan to revisit the policy regularly in the light of ever-changing technologies and to ensure the issues covered are understood by all pupils and staff.



Schools' E-Safety Policy 2006

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of ICT.

When thinking about the areas of risk, it might be useful to remember the four Cs.

- Content – exposure to age inappropriate material, inaccurate or misleading information, socially unacceptable material (eg inciting violence, hate or intolerance) and illegal material (eg images of child abuse).
- Contact – grooming using communication technologies leading to sexual assault and/or child prostitution.
- Commerce – exposure to inappropriate advertising, online gambling and financial scams.
- Culture – bullying via websites, mobile phones or other communications technologies. The downloading of copyrighted materials, such as music and films may involve children in illegal activities.

This template has been produced to help schools write their own e-safety policy. To encourage debate, the template offers a range of responses to common questions.

Many individual schools and LAs across the UK have used earlier editions of the Kent policy template. They incorporated experience gained since the first version was adopted, recent initiatives and advice from child protection officers. Further advice and contributions from Becta, members of NAACE, colleagues in the South East Grid for Learning and the British Computer Society Schools Expert Panel have also been included. This version has been further updated and adapted for schools within Bracknell Forest.

Where a statement is marked ***BF Rec*** we particularly recommend that you include it, or a similar form of words adapted to suit your context, in your e-safety policy. The importance of these statements may not always be immediately obvious but have resulted from previous legal cases or other legal advice.

Core Principles of E-Safety

The internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of pupils.

A recommended e-safety policy is built on the following three core principles:

Educating young people to be responsible users of ICT

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must also learn how to recognise and avoid these risks for themselves as they grow older – to become “internet wise”. The precise nature of the risks faced by young people will change over time as new technologies, fads and fashions take hold, but there are general principles of safe online behaviour that apply to all sorts of situations, eg. pupils need to know how to react if they come across inappropriate material and that they should not give out personal information such as their address and telephone number to strangers or publish this on the internet. They should also be educated to critically evaluate the quality of the material they find on the internet.

The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Guided educational use

Significant educational benefits should result from curriculum ICT use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum ICT use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful ICT use will also reduce the opportunities for activities of dubious worth.

Regulation and control

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones.

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

This document describes strategies to help to ensure responsible and safe use. They are based on developing responsibility, guiding pupils towards educational activities and limiting access. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

A School E-Safety Policy

(A template for schools to edit)

1 Who will write and review the policy?

Possible statement:

- *Our e-safety policy has been written by the school, building on the Kent NGfL policy, Bracknell Forest LA ICT Advisory Group recommendations and government guidance. It has been agreed by the senior management and approved by governors following discussions with the PTA and Student Council. It will be reviewed annually.*

Created by:

Date:

To be revised:

Approved:

2 Why is internet use important?

Possible statements:

- *The purpose of 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 information and business administration systems.*
- *Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.*
- *Internet access is an entitlement for students who show a responsible and mature approach to its use.*
- *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.*

3 How does the internet benefit education?

Possible statement:

Benefits of using the internet in education include:

- *Access to world-wide educational resources including museums and art galleries;*
- *Inclusion in government initiatives such as the DfES ICT in Schools*
- *Educational and cultural exchanges between pupils world-wide;*
- *Cultural, vocational, social and leisure use in libraries, clubs and at home;*
- *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 including remote management of networks;*
- *Exchange of curriculum and administration data with the LA and DfES.*
- *Mentoring of pupils and provide peer support for them and teachers*

4 How will internet use enhance learning?

Possible statements:

- *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.*
- *Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.*
- *Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.*
- *Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, evaluation and retrieval.*

5 How will pupils learn to evaluate internet content?

Possible statements:

- *If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.*
- *Schools should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.*

The following statements will require adaptation according to the pupils' age:

- *Pupils should be taught to be critically aware of the materials they read and 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.*

Training should be available to staff in the evaluation of web materials and methods of developing students' critical attitudes.

6 How will e-mail be managed ensuring safety for pupils?

Possible statements:

- *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 details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.*
- *Personal email or messaging between staff and pupils should not take place.*
- *Whole-class or group e-mail addresses should be used at Key Stage 1 and below.*
- *Access in school to external personal e-mail accounts may be blocked.*
- *Excessive social e-mail use can interfere with learning and may be restricted.*
- *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.*

7 How should website content be managed?

Possible statements:

- *The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.*
- *Web site 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 website, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.*
- *The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.*
- *The website should comply with the school's guidelines for publications.*
- *The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce it has been obtained.*

8 Newsgroups, e-mail lists and forums

Possible statements:

- *Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.*
- *Access to forums that are moderated by a responsible person or organisation and are directly linked to an educational activity will be permitted.*

9 Chat and instant messaging

Possible statements:

- *Pupils will not be allowed access to public or unregulated chat rooms.*
- *Pupils will not access social networking sites for example 'My Space' or 'Bebo'.*
- *Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.*
- *Any form of bullying or harassment is strictly forbidden.*
- *A risk assessment will be carried out before pupils are allowed to use a new technology in school.*

This statement relates to an employment tribunal decision:

- **BF Rec* Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone. Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.*

10 Personal websites and blogs

Possible statements:

- *Pupils will not access social networking sites for example 'My Space' or 'Bebo'.*
- *When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.*

11 Photographic, video and audio technology

Possible statements:

- *When not in use, video conferencing cameras should be switched off and turned to face a wall.*
- *It is not appropriate to use photographic or video devices in changing rooms or toilets.*

- *Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.*
- *Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities.*
- *The downloading of audio or video files is not permitted, without the prior permission of the network manager.*
- *Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.*
- *Pupils should always seek the permission of their teacher before making audio or video recordings within school.*

12 How can emerging ICT applications be managed?

Possible statements:

- *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.*
- *Mobile phone cameras should not be used inappropriately and photographs should not be forwarded to unknown sources.*
- *The use of blog messaging on social network sites is strictly forbidden.*

13 How will internet access be authorised?

Possible statements:

- *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.*
- *At 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 informed that pupils will be provided with supervised internet access (an example letter for primary schools is included as an appendix).*
- *Secondary students must apply for internet access individually by agreeing to abide by the Responsible Internet Use statement. Parents will be asked to sign and return a consent form. Please see the sample form later in this document.*
- *Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.*

14 How will the risks be assessed?

Possible statements:

- *In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. 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 Bracknell Forest Borough Council can accept liability for the material accessed, or any consequences of 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 minimise risks will be reviewed regularly.*
- *The headteacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.*
- *Access is strictly forbidden to any websites that involve gambling, games or financial scams .*

15 How will filtering be managed?

Possible statements:

- *The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.*
- *If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.*
- *Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- *Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk) .*
- *Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.*

16 How will the policy be introduced to pupils?

Possible statements:

- *Rules for internet access will be posted in all rooms where computers are used.*
- *Pupils will be informed that internet use will be monitored.*
- *Instruction in responsible and safe use should precede internet access.*
- *A module on responsible internet use will be included in the PSHE programme covering both school and home use.*

17 How will staff be consulted and made aware of this policy?

Possible statements:

- *All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.*
- *All new staff will be taken through the key parts of this policy as part of their induction.*
- *All new staff will be provided with a copy of this policy.*
- *All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School e-Safety Policy, and have its importance explained.*
- **BF Rec* Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.*
- *The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.*
- *Staff development in safe and responsible internet use, and on the school internet policy will be provided as required.*
- *Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.*

18 How will ICT system security be maintained?

Possible statements:

- *The school ICT systems will be reviewed regularly with regard to security.*
- *Virus protection will be installed and updated regularly.*
- *Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.*
- *Personal data sent over the internet will be encrypted or otherwise secured.*
- *Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.*
- *Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.*
- *Files held on the school's network will be regularly checked.*
- *The IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by internet use.*

19 How will complaints regarding internet use be handled?

Possible statements:

- *Responsibility for handling incidents will be delegated to a senior member of staff.*
- *Any complaint about staff misuse must be referred to the headteacher.*
- *Pupils and parents will be informed of the complaints procedure.*
- *Parents and pupils will need to work in partnership with staff to resolve issues.*
- *Sanctions available include:*
 - *interview/counselling by head of year;*
 - *informing parents or carers;*
 - *removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.*
- *As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies. Advice sought should include how best to preserve any possible evidence.*

20 How will parents' support be enlisted?

Possible statements:

- *Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school website.*
- *Internet issues will be handled sensitively to inform parents without undue alarm.*
- *A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.*
- *Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (web addresses in reference section).*

21 How is internet used across the community?

Example of internet access rules in libraries:

- *Adult users will need to sign the e-safety policy or alternatively an acceptable use policy.*
- *Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.*
- *In libraries, generally children under 8 years of age must be accompanied by an adult when accessing the internet.*