

Rationale/Philosophy:

The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Aims and Objectives:

The School's Internet Access Policy is part of the school's Information and Communication Technology (ICT) Policy and ICT Development Plan and will relate to other policies including those for behaviour and for personal, social and health education (PSHE) including citizenship.

The policy includes:

Appendix 1, The guidance for school "Child protection and the use of the Internet" as produced by the Pupil Support division of the local authority.

Appendix 2 Rules for Responsible Internet Use

Appendix 3 statement for inclusion in a communication with parents about safe use of the internet

Appendix 4 Internet usage permission letter and form

Appendix 5 Out of Hours learning

Appendix 6 Staff: Acceptable Internet Use Statement

The Internet Access Policy has been agreed by the staff in the school and approved by governors.

Implementation/Tasks:

Teaching and learning and the Internet

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers will plan for and make use of communications technology, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop life skills in their use.

Pupils will be taught:

- ways to validate the authenticity of information before accepting that it is necessarily accurate;
- to acknowledge the source of information, when using Internet material for their own use;
- that the writer of an e-mail or the author of a Web page might not be the person claimed;
- to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Rules for Internet access will be posted near computer systems (see Appendix 2)

Internet access

- Cambridgeshire Local Education Authority, through ICT Services will provide Internet access. There is a secure 'firewall' linked to the Cambridgeshire IT Service, which gives a limited access to the World Wide Web.

To ensure safe Internet access:

- Access will be granted to a whole class as part of the scheme of work, after a suitable education in responsible Internet use;
- Pupils will be informed that Internet use will be supervised and monitored;
- Parents will be informed that pupils will be provided with supervised Internet access;
- Pupils will not be allowed to access public chat rooms;
- The school will work in partnership with parents and the Local Education Authority to ensure systems to protect pupils are reviewed and improved;
- Staff will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice;

- New facilities for the future, such as video conferencing, will be thoroughly tested before pupils are given access.

E-mail management

The following principles will apply in respect of e-mail:

- E-mail must only be used in school for educational purposes;
- Pupils may send e-mail as part of planned lessons but will not be given individual e-mail accounts;
- In-coming e-mail will be regarded as public. Received e-mail may be examined by staff
- Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper;
- Forwarding of chain letters will be banned, as will the use of chat lines / rooms

Web site principles:

- The point of contact on the website is the school address, office email and school telephone number. Home information or individual e-mail identities are not published;
- Photographs will not normally identify individual pupils by their full name. Group shots or pictures taken over the shoulder will be used in preference to individual "passport" style images. Photographs of pupils will not be used without prior written permission and permission sought for photographs will be part of the annual data collection each September.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.

Risk assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. The school cannot accept liability for the material accessed, or any consequences thereof.

The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed and staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.

Tapestry - on-line learning

Tapestry will be used to share photographs and learning with parents as part of an on-line learning platform. Again permission will be sought and parents will need to sign their agreement to only use photographs on the site for personal use and not to be shared in a wider context. If a parent fails to use Tapestry in an appropriate manner, respecting the images and the school's policy regarding the use of Tapestry, a parent may be blocked from the use of this on-line learning tool.

Security of school ICT systems

The Internet is a connection to the outside world that could compromise system performance or threaten security. The system is maintained as follows:

- Security strategies are discussed with the LA;
- The IT co-ordinator ensures that the system has the capacity to take increased traffic caused by Internet use;
- The security of the whole system will be reviewed with regard to threats to security from Internet access;

- Personal data held by the school and sent over the Internet is encrypted or otherwise secured;
- Virus protection is installed and updated regularly;
- Use of floppy disks, CD Roms and memory sticks will be reviewed. Children's personal floppy disks, CD Roms and or memory sticks may not be brought into school without specific permission and a virus check;
- Use of e-mail to send attachments such as system utilities (ie operating system files) is not permitted

References:

- National Association for Co-ordinators and Teachers of IT, Acceptable Use Policy
- Internet Safety:
- Guidance on Access and the Safe Use of School IT equipment Cambridgeshire County Council
- www.teachernet.gov.uk
- DfES "Superhighway Safety" pack to our Year 3/4/5 and 6 pupils.
- Check government advice and recommendations found at <http://safety.ngfl.gov.uk>.
- www.becta.org.uk

Review: 3 yearly

Links to other relevant policies:

All subject policies

Signed:
(on behalf of P & CC)

Date:

Appendix 1 Guidance to all schools and educational establishments

CHILD PROTECTION AND THE USE OF THE INTERNET

1.0 Introduction

- 1.1 The government, the Local Authorities and schools are encouraging the use of the Internet to promote learning in a wide range of areas. Young people hardly need to be persuaded to learn in this way.
- 1.2 This document will refer to schools and teachers. However, the guidance contained here is applicable to many other Education settings, such as After-school clubs and all adults who supervise children in these settings. See Appendix 5

This guidance focuses on the personal safety and well being of pupils in our school. It sets out a number of points to clarify the potential risks and steps that staff can take to minimise those risks.

2.0 Our Teaching Programme

- 2.1 Learning to use the resources of the Internet safely and appropriately is an important part of the education of all pupils. We will incorporate Internet safety into the curriculum¹ and at the beginning of every term.
- 2.2 ¹ *Staying Safe is the Personal Safety Programme produced by and available from the Education Child Protection Service (Combs. LEA tel. 01480-375888). It contains useful information and resources to teach children about the safe Internet use. Staying Safe is aimed at Primary aged children, but can be adapted easily for use with children in Years 7 and 8 in secondary schools. It can also be adapted for use with children with special needs across primary and secondary settings.*
- 2.3 We will share with parents the steps that the school is taking to promote Internet safety and to involve them in discussion about what constitutes safe use both at school and at home.
- 2.4 Access to online resources will enable pupils to explore thousands of libraries, databases and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages.
- 2.5 Child friendly search engines ie Yahoo / Jeeves for Kids must be used in preference to adult search engines ie Google / Yahoo

3.0 Monitoring Internet Use

- 3.1 Cambridgeshire County Council is our Internet provider. Through Broadband everyone has equal open access to the World Wide Web. Cambridgeshire provide a filter and regularly check websites for suitability for school use. However, this is ongoing and if any member of staff or pupil finds access to an

inappropriate site then the ICT Coordinator and or Head must be informed immediately. The Head will then inform Cambridgeshire to enable them to deny access. Caution is therefore crucial and staff must check sites before enabling their pupils' access to these.

3.2 The most serious risk to pupils using the Internet involves the possibility of someone being hurt, exploited or abused as a result of personal information being posted online. The Police have a number of examples of cases such as these. Online pictures, names, addresses, ages or information about a child's likes or dislikes can be used to trace, contact and meet a pupil with the intention of causing harm.

3.5 The risk to children may not be immediate, since there can be a long period of building up a relationship known as the 'grooming process'.

3.6 On no account should either first names or surnames be attached to photos of children on websites.

3.7 If a website includes a child's photo, this could be downloaded from the web and edited in an unpleasant or embarrassing way. This new image could be circulated on other webpages.

3.8 Our school website should therefore not include close-up full frontal photos of children. All photographs of children should be general. Photos should be taken in such a way as to ensure that the individual identity of a child is protected (e.g. from an angle, in profile, at a distance, etc.)

3.9 Pupils will be taught to check with their teacher or supervising adult before providing any personal information that may be requested by a specific website. Teachers and supervising adults should know how to look at web page addresses and other information in order to assess the validity of a website. Pupils should understand never to divulge anyone else's personal information and only to supply minimal untraceable details, such as a first name, or only use initials to an enquiring website.

4.0 Using E-mail and Newsgroups and Social Media ²

4.1 Each member of staff will have their own email accounts and access to the Cambridgeshire portal. At this time the school does not offer pupil's email accounts, however if this was to be made available to pupils in the future:

4.2 It is essential for all e-mails sent and received by pupils to be monitored by supervising staff.

4.3 At Eynesbury our approach to a pupil or colleague who sends inappropriate e-mails should be clear and effective in halting such practice. It should also be seen to be effective.

4.4 Eynesbury School views social media as a home-leisure pursuit. As the use of the Internet for educational purposes increases in the classroom, a broader range of channels of communication is likely to develop. Therefore, the development of social media use in schools is likely in the future. At this time of reviewing the policy we do not see social media sites as an educational resource.

² *Newsgroups and social media are not generally available to Cambridgeshire schools who use the County Council as their Internet provider.*

Downloading Software

The Internet is known to contain illegal software (including data). Under no circumstances may illegal software be loaded onto County Council computer systems. In particular, but without limitation, the following activities are prohibited:

- requesting or downloading of any offensive, obscene or indecent images, data or material, or any data capable of resolving into the same
- requesting or downloading of defamatory material
- requesting or downloading of material which may infringe the copyright of another party
- deliberate activities with any of the following characteristics:
 - wasting staff or network resources.
 - corrupting another user's data
 - violating the privacy of other users
 - disrupting the work of other users
 - using the network in a way which may deny access to other users (e.g. deliberate or reckless overloading of access links or of switching equipment).

If you are unsure about the status of any material, check with the Head teacher and or ICT Coordinator, *before* you download it.



APPENDIX 2

Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- ❖ I will not access other people's files;
- ❖ I will only use the computers for school work and homework;
- ❖ I will not bring in floppy disks, CD Roms or memory sticks from outside school unless I have been given permission;
- ❖ I will ask permission from a member of staff before using the Internet;
- ❖ I will only e-mail people who my teacher has approved;
- ❖ The messages I send will be polite and responsible;
- ❖ I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- ❖ I will talk to an adult about anything I don't understand or find upsetting. I understand my discussion would be confidential and would help protect other pupils and myself;
- ❖ I understand that the school may check my computer files and may monitor the Internet sites I visit.

APPENDIX 3



Statement for inclusion in a communication with parents about safe use of the Internet - Annual Permission Slip - Year _____

Eynesbury School makes every effort to minimise the safety risks to children using the Internet in school. The most serious risk to children involves the possibility of someone being hurt, exploited or abused as a result of personal information being posted online.

Staff take their responsibilities very seriously in supervising Internet use of this kind.

We do not allow pupils to post personal information on the web such as their names, addresses, likes and dislikes. Similarly, photos of individual children are not allowed. Such information can be used to trace, contact and meet with pupils with the intention of causing harm. Our personal safety curriculum teaches children about the safe use of the Internet to protect themselves from potential harm of this kind.

We would strongly urge you as parents to adopt a monitoring role at home to children's use of the Internet. Remember that contact with individuals via 'Chatrooms' can potentially open children to exploitation by adults who may seek to harm them. We advise you to become aware of who your child is in contact with via the Internet, and to encourage your child to tell you if they come into contact with anyone who makes them feel uncomfortable.

We look forward to working with you to protect your child.

Yours etc.



APPENDIX 4

Internet use permission letter YEAR _____

Dear Parent,

Use of the internet and email in school

As part of the school's information and communications technology (ICT) programme, we offer pupils supervised access to the internet and email. Before the school allows students to use these facilities, they must obtain parental permission. Both pupils and parents must sign and return an Internet Use Permission Form as evidence of their acceptance of the school's Rules for Responsible ICT Use. Copies of both are enclosed with this letter.

Various projects have proven the educational benefits of internet and email access, which enable pupils to explore a wide range of information sources, and communicate and collaborate with other learners throughout the world. Although there are concerns about children having access to inappropriate material via the internet, the school takes a range of measures to minimise these risks. A filtering system is in operation which restricts access to inappropriate materials, and this is supplemented by an internet safety programme for all pupils which teaches the safe and appropriate behaviours to adopt when using the internet, email and other technologies.

Although internet use is supervised and filtered within our school, families should be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal, or potentially offensive to some people. As with any other area, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources at home. The school therefore supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.

If you agree for your child to use supervised internet access, please read the enclosed Rules for Responsible ICT use, discuss with your child, complete and sign the enclosed permission form and return it to me by the end of term. The school has a number of leaflets from national bodies that explain issues further and also cover internet use at home. If you would like copies of these, please contact the school. Should you wish to discuss any aspect of internet use, or to see a lesson in operation, please telephone the school to arrange an appointment.

Yours sincerely



Internet and email use permission form

Please complete and return this form to the Headteacher.

Pupil:

I have read and understand the school Rules for responsible **ICT** Use, and agree to comply with them. I will use the **Internet**, email and other **ICT** facilities at school in a safe and responsible way and follow our school rules for using the internet.

Pupil's signature _____

Date: ___/___/___

Parent:

I have read and understand the school Rules for responsible **ICT** Use, and as the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the **internet**, email and other **ICT** facilities at school. I understand that the school will take reasonable precautions to ensure that pupils can not access inappropriate materials, including the teaching of **internet** safety skills to pupils, but accept that ultimately the school can not be held responsible for the nature and content of materials accessed through the **Internet**. I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.

Parent's signature _____

Date: ___/___/___

Pupil's name _____

Form/class _____

Home Telephone _____



APPENDIX 6

Eynesbury CE (C) Primary School

Staff: Acceptable Internet Use Statement

The computer system is owned by the school and is made available to the staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school.

- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor the Internet sites visited.
- Email access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems or that attacks or corrupts other systems is forbidden.
- All Internet use should be appropriate to staff professional activity or to students' education.
- The school reserves the right to examine or delete any files that may be held on Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed if inappropriate sites are visited.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Legitimate private interests may be followed, providing school use is not compromised.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Staff requesting Internet and email access should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Coordinator for approval.
- If I am unsure about the status of any materials or software, I will check with the Headteacher or ICT leader.
- I will check web sites and search engines before using with pupils

Full name

Position

Signed

Access granted **Date**

Internet Safety - a checklist for school managers

Have your school managers considered the advice on internet safety provided by the government, the LA and other relevant authorities?

Does your provider employ a filtered internet feed and other security measures?

Does your school have a policy on internet safety which is understood and implemented consistently by all the staff who may use the internet?

Does your policy address:

- use of e-mail
- use of the worldwide web
- use of search engines
- use of pupils' names
- use of pictures of pupils
- supervision of pupils
- the role of parents

Have all staff who may use the internet received training and guidance on internet safety issues?

Do all staff fully understand the security features which your internet service provider employs?

Have pupils been involved in the development of an acceptable use policy?

Do all pupils understand their responsibilities when they are using the internet?

Do all pupils understand what they should do if they encounter something inappropriate when using the internet?

Have parents given informed consent to use of the internet by their children in accordance with your policy?