E-Safety Policy

Doc reference:	Issue:	Pages:	Author:	Status:
NP/0002	**2**	**12**	**Chris Williams**	**Approved**

Approved:	I. Ivens (Chair: Curriculum & Standards Committee)	Date: 2 July 2013
Reviewed:	(Signatures)	

Contents List

Document history

Issue 1: This is a new policy written in February 2009.

Issue 2: This policy has some minor modifications (October 2012).

1 Introductory statement

The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.

The dangers associated with the Internet and emerging new technologies are highly publicised in the media e.g.

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.

- Children might receive unwanted or inappropriate messages from unknown senders via email or via files sent by Bluetooth. They might also be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites. Chat rooms provide cover for unscrupulous individuals to groom children.

Despite these dangers, however, there are social and educational benefits to be derived. E.g.

- Children are equipped with skills for the future.
- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, Instant Messaging and Social Networking helps to foster and develop good social and communication skills.

We believe that these benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

This policy, written in accordance with BECTA guidelines, focuses on the use of the internet and email and outlines the procedures in place to protect users and the sanctions to be imposed if these are not adhered to.

2 Procedures for use of a shared school network

Users must access the school network using their own logons and password, where these are used. These must not be disclosed or shared.

Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.

Software should not be installed, nor programmes downloaded from the Internet without prior permission of the ICT Co-ordinator.

Removable media (e.g. pen drives / memory sticks, CD-ROMs) must be scanned for viruses before being used on a machine connected to the network.

Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').

Machines must be 'logged off' correctly after use.

3 Procedures for use of the internet and email

All users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment.

Parental or carer consent is requested in order for children to be allowed to use the Internet or email.

Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account.

The Internet and email must only be used for professional or educational purposes.

Children must be supervised at all times when using the Internet and email.

Procedures for Safe Internet use and sanctions applicable if rules are broken will be clearly displayed In classrooms and the ICT suite.

Accidental access to inappropriate, abusive or racist material is to be reported without delay to the ICT Co-ordinator and a note of the offending website address (URL) taken so that it can be blocked.

Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.

Internet and email use will be monitored regularly in accordance with the Data Protection Act by the ICT Co-ordinator.

Email addresses assigned to individuals are in a form which makes them easily identifiable to others. For this reason, children are only permitted to email within school.

Users must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.

All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

All emails sent from a school email account will carry a standard disclaimer disassociating the school and the Local Authority with the views expressed therein.

Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes.

Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

All email with attachments received from unknown senders, and/or if the content of the attachment is not detailed in the body of an email, should not be opened, but subsequently deleted.

Users must seek the permission of the ICT Co-ordinator before downloading any files from the Internet.

All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.

4 Procedures for use of cameras, video equipment and webcams

Permission must be obtained from a child's parent or carer before photographs or video footage can be taken.

Photographs or video footage will be downloaded immediately and saved into a designated folder. This will be 'password-protected' and accessible only to authorised members of staff and children when supervised. Photographs/videos must be deleted from the camera as soon as they have been downloaded.

Any photographs or video footage stored must be deleted immediately once no longer needed.

Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a 'password-protected' folder onto a school computer immediately upon their return and deleted from the device.

5 Procedures to ensure safety of the school's website

The Headteacher and ICT Co-ordinator are responsible for approving all content and images to be uploaded onto its website prior to it being published.

The school website should be subject to frequent checks so ensure that no material has been inadvertently posted, which might put children or staff at risk.

Copyright and intellectual property rights must be respected.

Permission must be obtained from parents/carers before any images of children can be uploaded onto the school website.

Names must not be used to identify individuals portrayed in images uploaded onto the school website. Only group shots are permissible. Similarly, if a child is mentioned on the website, photographs which might enable this individual to be identified must not appear.

When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names.

6 Procedures for using mobile phones and personal digital assistants (pdas)

Children are not permitted to bring mobile phones into school. Staff are required to switch mobile phones off during lesson times.

The taking of still pictures or video footage without the subject's permission is not ethical, so will not be permitted.

7 Procedures for using wireless games consoles

The use of wireless games consoles is not permitted and should not be brought into school.

8 Sanctions to be imposed if procedures are not followed

Cases of misuse will be considered on an individual basis by the Network manager and Headteacher and sanctions agreed and imposed to 'fit the crime.' These may include:

- Letters may be sent home to parents/carers (if applicable).
- Users may be suspended from using the school's computers, Internet or email, etc. for a given period of time / indefinitely.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

9 Concluding statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and that this policy will not remain static. The use of any emerging technologies will be permitted upon completion and approval by the Network manager and Headteacher of a risk assessment, which will be used to inform future policy updates.

10 APPENDIX 1 – Acceptable Use Agreement (AUP) for Pupils

Hollingworth Primary and Nursery School

Acceptable Use Agreement for the Internet, Email and other technologies

In order for pupils to browse the Internet or make use of Email and other technologies, we require each child (and their parent or carer) to sign to show that they understand the importance of adhering to these strict rules:

- I will only use the Internet when I have permission and I am supervised.
- I will only send emails to people my teacher has approved. I understand that racist or bad language will not be tolerated and my emails will be polite at all times. I will not use email as a way to bully another child or adult.
- I will not give out my address, home or mobile telephone number, photograph or school name and address on the Internet or in an email. I will not give out personal details of another child or adult either.
- I agree never to meet someone I communicate with through email and I will tell a teacher, parent or carer straightaway if a stranger tries to contact me on the Internet or by email.
- I will tell my teacher straightaway if I come across any unsuitable pictures or information on the Internet by accident or if anything makes me feel uncomfortable or upset.
- I will only use search engines or websites that have been chosen by a teacher. I will not try to access any inappropriate websites, chat rooms, Instant Messaging or Social Networking sites in school.
- I agree that if I bring a mobile phone or other device into school, they MUST be left in the office during the school day.
- I will not download any files from the Internet in school unless I have permission.

Pupil

I understand the rules above and agree to follow them. If I break any of these rules, I understand that:

1. A letter might be sent home;
2. I might be banned from using the Internet for a given period of time.
3. More serious action might be taken.

Pupil Signature: _____

Date: ___/___/___

Parent or Carer

I give permission for my child to use the Internet, email and other technologies in school. I understand that pupils will be held accountable for their own actions and agree to appropriate sanctions being imposed if rules are broken. I am aware that some materials on the Internet may be offensive and I accept responsibility for setting standards for my child to follow when selecting, sharing and exploring information and media.

Name of Pupil: _____

Parent/Carer Signature: _____

Date: ___/___/___

11 APPENDIX 2 – Acceptable Use Agreement (AUP) for Staff

Hollingworth Primary School

Internet Acceptable Use
Guidelines for Staff

Introduction

The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school. Staff and students requesting Internet access should read and sign a copy of this Acceptable Use Statement and return it to the IT Manager for approval.

All members of staff are responsible for explaining the rules for Internet usage and their implications. All members of staff need to be aware of possible misuses of online access and their responsibilities towards pupils.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited and e-mail sent or received. Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

Acceptable use

As a general principle Internet access is provided to support work-related activities. The following guidelines apply:

- All Internet activity should be appropriate to staff professional activity, including teaching, research, administration and management, or the student's education
- Access should only be made via the authorised accounts and passwords, which should not be made available to any other person

Unacceptable use

The following uses will be regarded as unacceptable

- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems
- Use for personal financial gain, political purposes, advertising, personal or private business
- Misuse of materials which have copyright
- Posting anonymous messages and forwarding chain letters
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material
- Illegal or malicious use

Disciplinary Action

- Violation of the above code of conduct will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- When applicable, police or local authorities may be involved.

I confirm that I have read the above Internet Acceptable Use guidelines. I understand that if I contravene the Guidelines, disciplinary action may be taken against me.

Full name	**Position in school (form)**
Signed	**Date**
Access granted	**Date**

12 APPENDIX 3 –Acceptable Use Guidelines for Guest Use

Hollingworth Primary School

Internet Acceptable Use
Guidelines for Guest Use

Introduction

The school's Internet Access Policy has been drawn up to protect all parties - the pupils, the staff and the school. Staff and students requesting Internet access should read and sign a copy of this Acceptable Use Statement and return it to the ICT Co-ordinator for approval.

All members of staff are responsible for explaining the rules for Internet usage and their implications. All members of staff need to be aware of possible misuses of online access and their responsibilities towards pupils.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited and e-mail sent or received. Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

Acceptable use

As a general principle Internet access is provided to support work-related activities. The following guidelines apply:

- All Internet activity should be appropriate to staff professional activity, including teaching, research, administration and management, or the student's education
- Access should only be made via the authorised accounts and passwords, which should not be made available to any other person

Unacceptable use

The following uses will be regarded as unacceptable

- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems
- Use for personal financial gain, political purposes, advertising, personal or private business
- Misuse of materials which have copyright
- Posting anonymous messages and forwarding chain letters
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material
- Illegal or malicious use

Disciplinary Action

- Violation of the above code of conduct will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- When applicable, police or local authorities may be involved.

I confirm that I have read the above Internet Acceptable Use guidelines. I understand that if I contravene the Guidelines, disciplinary action may be taken against me.

Full name	Position in school (form)
Signed	Date
Access granted	Date

Risk Assessment Pro-forma for Emerging Technologies