E-Safety Policy

Doc reference:	Issue:	Pages:	Author:	Status:
NP/0002	**1**	**8**	**Chris Williams**	**Approved**

Approved:	K. Johnson (chair: curriculum & standards committee)	Date:
Reviewed:	(Signatures)	(Dates)

Contents List

Document history

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

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.

1.1 Use of email, mobile phones, Internet messaging and blogs all enable improved communication and facilitate the sharing of data and resources.

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 Network manager.

Removable media (e.g. pen drives / memory sticks, CD-ROMs and floppy disks) 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 beside every computer with access to the Internet.

Accidental access to inappropriate, abusive or racist material is to be reported without delay to the Network manager 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 Network manager.

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 Network manager 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. 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.

5 procedures to ensure safety of the school's website

The Headteacher and Network manager 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. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.

***Important:** It is perhaps safer not to post images of individuals (especially where children are concerned) onto the school's website, but to insist instead that only group photographs are used. If you opt for this approach, you must state this in your policy and ensure that all staff are aware of this procedure and consequently adhere to it.

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 Procedures for using portable media players (e.g. ipods)

The use of portable media players (e.g. iPods) is not permitted and should not be brought into school.

9 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.

10 Concluding statement

That 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.

11 Appendix

Acceptable Use Agreement (AUP) for Staff

Acceptable Use Agreement (AUP) for Pupils

Acceptable Use Agreement (AUP) for Guest Use

Risk Assessment Proforma for Emerging Technologies