

Advice to Headteachers on the use of Internet Technology

These guidelines should be used in association with City and County of Swansea Local Education Authority **BROADBAND NETWORK USE AGREEMENT** September 2003.

1. Introduction

- 1.1 Schools should adopt the following safeguards, which will enable children and staff to work within a reasonably 'safe' environment.
- 1.2 If the school introduces them as part of an educational process it will develop a culture for Internet use which will serve children and staff beyond the confines of the school.
- 1.3 The following guidelines should provide sufficient coverage to adapt for the creation of your own school policy. Where schools have policies in place already, they could provide a benchmark to evaluate that all necessary points are covered in your own policy.

2. Rules and Regulations

- 2.1 Every school should have an Acceptable Use Policy for the Internet. All Governors and Staff should be familiar with the policy and the school may wish to share this with parents to put them at their ease and to consider whether they wish to implement it at home.
- 2.2 The responsibility for its implementation lies with the governing body and headteacher, not the ICT Co-ordinator or Head of ICT.
- 2.3 The school should consider the use of a 'contract' for use with each pupil which is signed by parents or guardians. It highlights the issues and responsibilities shared.
- 2.4 Rules and Regulations should be made explicit.
- 2.5 It may be appropriate for an adaptation of the Acceptable Use Policy to be a home page on each station and pupils have to click an "accept" button in order to access the Web and e-mail.

3. Systems

- 3.1 Content and Site Filtering. All schools should employ filtering software or contract others to do this on their behalf. This software can filter known sites containing unsuitable materials and key words. The Authority uses Websense. But, filtering software should not be relied upon as a total solution.
- 3.2 Schools should employ a monitoring system to check on Internet usage.

4. Design and Deployment of Facilities

- 4.1 Computers or televisions which access the Internet should be deployed in open or busy areas which are easily supervised. They should not be located in closed or hidden areas.
- 4.2 Wherever possible computer rooms should be designed so that screens face into rooms where they are easily seen and supervised. The practice of placing computers in islands to squeeze in more stations is discouraged. If unavoidable, strategically placing mirrors might be a cheaper if less effective option.

5. Induction

- 5.1 Pupils will need to be properly prepared prior to their use of the Internet and this is perhaps best done as part of the school's normal learning programmes. Induction should include the development of basic Internet skills together with an understanding of the protocols, ethics and dangers.

6. Supervision

- 6.1 It is imperative that pupils are supervised in their use of the Internet. This cannot be overstated. It is the most effective way to protect children and to monitor their behaviour. No child should have access without proper supervision.

7. Deterrent

- 7.1 Pupils and staff must be made aware of the seriousness of Internet misuse. Staff must be fully aware of their responsibilities and the real dangers and consequences which might occur. Breaches will be subject to Child Protection Procedures.
- 7.2 Following proper supervision and monitoring practices, Heads should emphasise the certainty of being observed and caught. This is a powerful deterrent.
- 7.3 Headteacher should also warn pupils that misuse of the Internet will be severely dealt with as part of the school's Internet Policy. The ability to undertake the necessary sanctions to deal with misuse must be considered.

8. Electronic Mail

- 8.1 Teachers should not let pupils make contact with others by e-mail without first ensuring that they know who the contact is. People at the other end are not always who they say they are. Paedophiles have been known to make contact with children by this method. Children should be encouraged to adopt the same attitude as they are taught about talking to strangers.

9. School Web Sites

- 9.1 If publishing children's work on the school's web site or on any other web site, do not show both the child's name and a photograph. If the photograph is shown, do not put more than their initials. Do not do anything that helps to identify them in a photograph. It is imperative that pupils' e-mail addresses are not published on a publicly accessible Web Site.

10. Reporting Procedures

- 10.1 Accessing undesirable materials can easily happen by accident. Clear reporting arrangement need to be established and pupils encouraged to inform their teacher. This is part of the culture that schools should aim towards.
- 10.2 Teachers should report incidents to the Headteacher.
- 10.3 Headteachers will need to make decisions about reporting incidents to the LEA.
- 10.4 The LEA will need to make decisions on whether to pass information on to the police.

11. Legal Implications

- 11.1 The law with regard to responsibility for allowing school property to be used to access illegal materials or other illegal use with regard to the Internet is unclear. Governors and Headteachers will need to consider the legal responsibilities in this regard.

Safer Use of the Internet

Key Stages 1 and 2

- 1) Pupils must not have access to the Internet passwords. If passwords are discovered by pupils then Internet use should be suspended until the password has been changed.
- 2) Pupils must always be supervised when working on the Internet.
- 3) Computers with Internet access must be placed in a well-monitored area and positioned so that the screen is visible.
- 4) All World Wide Web sites must be checked by the teacher for appropriate content prior to use with pupils.
- 5) Suitable sites should be book-marked.
- 6) All Internet use should be through directed, focused tasks.
- 7) Internet access must be closed when the lesson ends.
- 8) Great care must be taken when using Internet Search Engines.
- 9) Teachers must carry out searches prior to the pupils using the same Search Engine and search parameters.
- 10) Close supervision is essential if Search Engines are used.
- 11) Gateways (sites which provide links to other sites) such as NGfL Cymru are preferable to Search Engines.
- 12) Pupils should be made aware that a record of their Internet use is held on the computer and Internet server.
- 13) If schools create Web sites, pictures of the pupils must not be published with their names.
- 14) Teachers and pupils must be aware of the potential dangers of e-mail, especially with regard to communicating with strangers.
- 15) Initial use of the e-mail facility should be confined to internal use only i.e. pupils communicate with each other.
- 16) If external contact is made initial e-mail contacts must always be made by the teacher.
- 17) All e-mail messages received must always be checked by the teacher first.
- 18) All unsolicited e-mail messages, especially those with attachments should be regarded as suspicious.
- 19) Teachers must be aware of the existence of copyright in all media.
- 20) Pupils must not pass personal details e.g. home telephone numbers or addresses to anyone over the Internet.

Safer Use of the Internet

Key Stages 3, 4 and post-16

- 1) The use of ICT is an essential part of most learning programmes. However, pupils must restrict themselves to usage which is both ethical and appropriate.
- 2) As at the earlier Key Stages, pupils using the Internet should be supervised and visited websites monitored.
- 3) At the higher levels, pupils will become more autonomous users of ICT, including their use of the Internet. Pupils should be encouraged to discuss terms and parameters to be used when searching for information, rather than be directed.
- 4) It is preferable that pupils use Internet portals or gateways to locate information rather than search engines. However, it is accepted that search engines will have to be used when no other means of locating information is available.
- 5) Wherever possible, teachers should check search engine results with parameters expected to be used by pupils to minimise the risk of inappropriate sites being returned.
- 6) Teachers must ensure, as far as is reasonably possible, that copyright laws are not infringed when pupils extract and save content from WWW sites.
- 7) Pupils must not attempt to download programs or executable files from the Internet without the express permission of a teacher. Similarly, pupils should not attempt to upload files or other material without permission.
- 8) When using e-mail, pupils must not use obscene or offensive language or use terms which may be considered insulting or inappropriate. Pupils must not impersonate another user, nor e-mail anonymously.
- 9) Casual use of the Internet (e.g. surfing) is not acceptable. Pupils' use should be directed to research based on the curriculum area or topic being studied. This also includes use of the Internet for commercial or for profit purposes.
- 10) Pupils at Key Stages 3 and 4 may require personal e-mail accounts. This should be left to the teacher's discretion and be given to those pupils deemed as being trustworthy. Pupils should be made aware that their e-mail messages may be checked.
- 11) No pupil should disclose any personal details, such as their home address or telephone number across the Internet.
- 12) Pupils must ensure that any website containing inappropriate materials is brought to the attention of the supervising teacher.
- 13) Pupils should be aware that materials they read whilst online may not be accurate.
- 14) It is highly recommended that pupils are directed to clear the computer's history of visited sites and empty the cache when they log off from an Internet session.

References

Acknowledgment is made to Neath and Port Talbot Borough Council in the drafting of this document.

A good link is Northamptonshire County Council which provides templates and suggestions for constructing your own acceptable use policy -

<http://www.northants-ecl.gov.uk/apps/ICT/dia/hme.asp>

The Government's guidelines on safe use with pupils provides a number of documents which can be accessed from - <http://safety.ngfl.gov.uk/schools/>

Two examples of school policies, both from the NGfL Cymru website, are Trinity Fields School http://www.ngfl-cymru.org.uk/internet_and_it.pdf

and Llangewydd Junior School in Bridgend

http://www.ngfl-cymru.org.uk/internet_policy.pdf

BECTa has guidelines at

<http://www.ictadvice.org.uk/index.php?section=ap&cat=004002&rid=463>