ARCHIBALD FIRST SCHOOL
E -SAFETY POLICY DOCUMENT

POLICY IMPLEMENTED: SEPTEMBER 2007, UPDATED AND REVIEWED: SEPTEMBER 2011

Contents

What is E-safety?

E-Safety encompasses the use of Internet technologies and electronic communications such as webcams, digital video equipment, mobile phones, camera phones, PDAs and portable media players. It highlights the need to educate pupils about the benefits, risks and responsibilities of using information technology as well as raising user's awareness of how to keep themselves safe using electronic technology.

Archibald First School will provide a framework for safe and appropriate use of the Internet and other technology. As a school we aim to create a safe ICT learning environment for the whole school community and to balance fulfilling the need to give pupils full access to resources with the need to protect them from unacceptable materials.

This policy will replace the current Acceptable Use Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.
The school's e-Safety policy will operate in conjunction with other school policies including those for behaviour and PSHCE and will be reviewed biannually.

Communications Policy
The E-Safety and Acceptable Use Policy will be thoroughly introduced to all staff, pupils and parents and its importance explained. All staff and other users are required to follow the conditions laid down in the policy. Users will be informed that Internet use is carefully monitored and that actions can be traced to an individual user. Staff should use ICT resources discretely and professionally.

In the case of employees breach of the conditions may constitute a breach of conditions of service and could lead to dismissal on the grounds of misconduct. Pupils breaching the conditions the following sanctions may be enforced:

- Temporary or permanent ban on Internet use.
- Additional disciplinary action in line with school behaviour policies
- Parents and other external agencies may be contacted.

The E-Safety rules will be visible by all computers and 'Keeping Up With children on the Internet…' from Childnet International will be sent home for parent information.

Teaching and Learning

ICT in schools is taught as a subject in its own right and also supports children's learning in across the entire curriculum. Within ICT lessons children learn to use a wide range of ICT including the Internet, email and digital cameras.

The Internet

Why Internet use is important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. The Internet gives staff and pupils access to a global network of information, including:

- A wider range of resources and materials which can enrich subject learning across all curriculum areas, as well as independent study and cross-curricular project work;
- Opportunities for world-wide communication with other pupils and teachers;
- Opportunities for the development of independent learning and research skills;
- Cultural, social and leisure information;
- A range of support services.

In addition it can lead to:

- Development of network literacy (i.e. the capacity to use electronic networks to access resources, create resources and communicate with others - these can be seen as complex extensions of the traditional skills of reading, writing, speaking and listening, awareness of audience);
- Social development.

The school Internet access will be designed expressly for pupils 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. All pupils will be taught the '5 smart rules' from Childnet International. The rules will be on display throughout the school.

Older pupils will also be taught how to evaluate Internet content as materials on the Internet vary hugely in quality: some materials are biased, inaccurate or misleading, either deliberately or unintentionally. Internet users will be taught the need to be aware of these issues and the need to exercise caution and judgement in their use of any material they find.

The school will ensure that copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Downloading of files is restricted to staff, or pupils under supervision.

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents and children must read the 'Acceptable ICT Use Agreement' before pupils can use ICT resources.
- Parents will be clearly informed that the use of the Internet is a statutory requirement.
- Parents will be asked to sign an 'opt out' form to indicate that they do not wish their child to the Internet.
- Parents will be asked to sign an 'opt out' form to indicate that they do not give permission for their child's image and/or work to be used on the school website and in school publications.
- The school will keep a record of all staff and pupils who are not granted Internet access and consent and / or permission for use of photographs. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access withdrawn.

Community use of the Internet

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed annually
- Virus protection will be updated regularly
- Staff must not attempt to install new software or devices as this is the responsibility of the LA ICT Services Support Team.

Managing filtering

- Newcastle LA's filtering system aims to protect pupils from obscene material and information relating to the misuse of drugs and the promotion of violence, intolerance, racism and extreme political and social views.
- The school will work with the LA ICT Services Support Team.to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.
- The LA ICT Services Support Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Complaints

Any complaints of Internet misuse will be dealt with by a senior member of staff. If a complaint is made about staff misuse then it shall be referred to the head teacher. Parents and pupils will need to work in partnership with staff to resolve any issues raised.

E-mail

- Pupils may only use approved e-mail accounts on the school system (VTLE).
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mails sent, by any pupil, to an external organisation should be authorised before sending.
- Staff will only use school email accounts for school business. Personal accounts will never be used for professional matters.

Social networking and personal publishing

- Children have access to a learning platform: the Newcastle Virtual Teaching and Learning Environment. This will be promoted to parents and pupils as a safe forum for social communications. All communication will be monitored by staff and pupils made aware of this. Pupils will sign an agreement to use this sensibly.
- The LA will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will agree through the Acceptable Use Policy never to give out personal details of any kind which may identify them and/or their location.
- All staff agree when signing the Staff Code of Conduct to behave in a professional manner when using such sites in their personal time and are solely responsible for ensuring a high level of personal security regarding their accounts. Social Networking Sites will never be accessed during school time.

The School Website

The school website is an ideal tool to communicate with current parents and pupils as well as the local community and to share the achievements of all those at Archibald.

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing pupil's images and work

Parents and carers are required to state that they do not give permission for their children's work and/or images of pupils to be electronically published. To

ensure pupil's safety images that include pupils will be selected carefully and pupils' full names will not be used anywhere in the website, particularly in association with photographs.

Electronic Communications

Mobile Phones

Pupils are not permitted to have mobile phones in school at any time. Pupils are aware of this fact and will be made aware of the effects and consequences of sending abusive or inappropriate text messages to others be it in or out of school time. If a mobile phone is brought onto the school premises it will locked safely in the school safe to be collected by a parent at the end of the school day.

Staff are not permitted to use a personal mobile phone during teaching time and will ensure that they are turned off. No images of children will ever be taken on a member of staff's mobile phone.

Digital Cameras

Staff and children regularly use digital cameras; for example to photograph events, capture pupils completing activities and to record achievements. School cameras are available for all staff and children to use. A personal camera will never be used to take photographs of pupils . Images of pupils will never be stored on any USB device but will only saved onto the school system and accessed using the remote access scheme.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.

Declaimer

The school will take all reasonable precautions to ensure that users access only appropriate material. However the school recognises that, under certain circumstances, the Internet can give staff and pupils access to undesirable information and images. We have done all that is possible to ensure children are protected from such information through the use of security software, a filtering system implemented by the LA ICT Services Support Team, limiting of features and construction of an Intranet and Website that provide as safe an environment as possible. The children are taught to use the facility sensibly and with proper consideration for others through the Internet Proficiency Scheme developed by BECTA and published by the DfES.
The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

References

Becta
www.ictadvice.org.uk

Ambleside C.E. Primary School
www.amblesideprimary.com

Kent County Council 2007

This policy is revised by Archibald First School based on the original Kent LA policy document.

SUMMARY OF THE 'ACCEPTABLE USE OF THE INTERNET'

Acceptable use of the Internet is characterised when teachers ensure that the computers, electronic communications equipment and the Internet may only be used for legal activity consistent with the aims, objectives and rules of the school. In particular the teacher should make sure that all users are made aware of the following rules.

Safety on the Internet and Responsible use of computers

Members of Staff

- *Realise that the use of pupil's names and work, and photographs of pupils will require the written permission from parents, guardians or carers.*

Members of Staff and Pupils

- *Only use your own network login and password, which is kept secret.*
- *Never bring software or disks into school without seeking permission from the ICT Team.*
- *Never open or reply to e-mails from strangers. All e-mails from unknown sources should be reported.*
- *Never e-mail your password, address, telephone number, or school name to someone else, especially strangers.*
- *Do not download, use or upload any material that is copyright. If you do not have the permission of the author/owner DO NOT USE THE MATERIAL.*
- *E-mails that make you unhappy or feel uncomfortable should be reported.*
- *Websites that make you unhappy or uncomfortable should be reported.*
- *Pupils should only use provided links by themselves (inclusive of gaming sites). The free use of the Internet, is not permitted, unless in the presence a member of staff.*
- *It is not permitted to use strong language, swearing or aggressive behaviour at anytime.*
- *Any incidents that breach the Acceptable Rules Policy should be immediately reported to an ICT co-coordinator or the Head teacher.*
- *In the interests of security, the school reserves the right to make a detailed log of all access to sites, including your Internet Service Provider and details of your computer system. Personal discs may also be checked for viruses and inappropriate material.*
- *All pupils and staff will pledge not to deliberately access unsuitable material and that, should any be found accidentally, will report it immediately to the ICT Team.*

Pupils

- *Meeting up with an e-mail contact is forbidden without parental permission.*
- *Pupils will have no access to newsgroups or chat rooms.*
- *Competitions or contests should not be entered into in school time and parental permission must be sought when using the Internet outside of school.*

If the rules are deliberately broken, it will result in discontinued use of the internet or computers.

UNACCEPTABLE USE OF THE INTERNET – PUPILS AND STAFF

Unacceptable use of the Internet is not tolerated. Pupils and staff should be aware that the following activities, whilst not an exhaustive list, are unacceptable:

- The access to or creation, transmission or publication of any offensive, defamatory, obscene or indecent images, sounds, data or other material. In the case of staff this can lead to prosecution by the police.
- The receipt or transmission of material such that this material infringes the copyright of another person or infringes the conditions of the Data Protection Act 1984.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Posting anonymous messages and forwarding chain letters is forbidden.
- The transmission of unsolicited commercial or advertising material to other Net users.
- The deliberate unauthorised access to facilities, services, data or resources via the Internet.
- Activities with the following characteristics or could result in the following characteristics:
  - wasting staff or other users efforts or network resources, including time on remote systems and the efforts of staff involved in the support of those systems ·
  - corrupting or destroying other users data
  - violating the privacy of other users ·
  - disrupting the work of other users · using the Internet in a way that denies service to other users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large image files)

Appendix: Legal and Ethical Issues

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The following acts can be related to electronic communications:

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
This Act introduces new offences of grooming, and in relation to making/distributing indecent images of children, raised the age of the to 18 years.

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor

communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network.
Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.
Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Archibald First School follows the guidance from the 'Fair Processing Notice' as received from the LA.