Alfriston School

E-Safety Policy & ICT Acceptable Use Policy

Policy reviewed: Sept 2016

Approved by Governors: Sept 2016

Next review: Sept 2017

CONTENTS PAGE

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.
Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home.

1. Core Principles of Internet Safety

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones.
There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

2. Why is Internet use 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 purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

3. How will Internet use enhance learning?

· The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
· Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
· Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. How will Internet access be authorised?

The school will keep a record of all staff and pupils who are granted Internet access.
The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
· Parents will be informed that pupils will be provided with supervised Internet access
· Primary pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
· There is a structured approach to internet access and internet searches, with clear progression through the school. This can be seen in the Computing planning overview.

5. How will filtering be managed?

· The school will work in partnership with parents, East Sussex County Council, to ensure systems to protect pupils are reviewed and improved.
· If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing subject leader or technician. Parents of the children involved will be notified immediately.
· Website logs will be regularly sampled and monitored by the ICT technician.
· Computing subject leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

6. How will the risks be assessed?

· In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. Teachers will preview and check material to be used in class. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor East Sussex County Council can accept liability for the material accessed, or any consequences of Internet access.
· The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
· Methods to identify, assess and minimise risks will be reviewed regularly.
· The Head Teacher and Computing subject leader will ensure that the Internet policy is implemented and compliance with the policy monitored.

7. Managing Content

7.1 How will pupils learn to evaluate Internet content?

· If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing subject leader
· Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
· Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
· Nominated persons (ICT technician) will be responsible for permitting and denying additional websites as requested by colleagues.

7.2 How should website content be managed?

· The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
· Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
· Pupils' full names will not be used anywhere on the website. No names will be used in association with photographs.
· Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

8. Communication

8.1 Managing e-mail

· Pupils may only use approved e-mail accounts on the school system.
· Pupils must immediately tell a teacher if they receive offensive e-mail.
· Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
· Whole-class or group e-mail addresses should be used.
· E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. It is recommended that staff also put their email communication in for approval before sending.

- Pupils and staff must keep their own logons and passwords private.
- Staff must use their school email account for official communications with outside bodies and with parents.

8.2 On-line communications and social networking.

· Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety.
· The school will conduct annual pupil surveys about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
· The use of online chat is not permitted in school, other than as part of its online learning environment.
-Staff are not permitted to link with pupils or former pupils via social networking sites. They are strongly discouraged from linking with parents of current or former pupils, as this may be seen as affecting their impartiality in cases of disputes between the school and parents or between parents.
-Staff are not allowed to make disparaging or unprofessional comments on pupils, staff, or any other school related matters on social networking sites.
-Staff should be aware of the risks of linking with other members of staff via social networking and be aware of the need to respect privacy.

8.3 Mobile technologies

· Appropriate use of mobile phones/ tablets etc will be taught to pupils as part of their e-safety programme. However mobile phones are not used in school at this time.
· Pupil mobile phones are not permitted within the school.
-Staff mobile phones are only permitted during official breaks and should be turned off at other times.
-Staff should not share their mobile phone number with parents or pupils.
-There is a school mobile phone for use on school trips. This number may be shared with parents.
· Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9. Introducing the Policy to Pupils

· Rules for Internet access will be posted in all rooms where computers are used.
· A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal

information safe, how to use mobile technologies appropriately and using online communication appropriately.
· Instruction on responsible and safe use should precede Internet access.
· Pupils will be informed that Internet use will be monitored.
· All Key Stage 1 & 2 pupils will undertake e-safety activities

10. Parents and E-Safety

· Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website.
· Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
· Internet issues will be handled sensitively to inform parents without undue alarm.
· A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
· All parents will receive support information as and when available, e.g. Know It All for Parents.

11. Consulting with Staff and their inclusion in the E-safety Policy

· All staff including teachers, supply staff, classroom assistants and support staff, will be provided with this policy, and its importance explained.
· The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
· All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
· Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
· Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.
· The school will adopt the Council's e-mail and Internet user policy.
· The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
· Staff development in safe and responsible Internet use will be provided as required.

12. How will complaints be handled?

· Responsibility for handling incidents will be delegated to a senior member of staff.
· Any complaint about staff misuse must be referred to the headteacher.
· Pupils and parents will be informed of the complaints procedure.
· Parents and pupils will need to work in partnership with staff to resolve issues.
· There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

13. Monitoring

All staff know and understand this policy, and as such, are made aware of the importance of regularly monitoring pupils' use of IT, and using IT sensibly themselves. The subject leader and Headteacher carry out an e- safety audit each year. This will include pupil, staff and parent surveys.

APPENDIX

Web-based Resources - For Schools

KidSmart http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

Childnet International http://www.childnet-int.org/
Guidance for parents, schools and pupils

Becta http://schools.becta.org.uk/index.php?section=is
e-Safety Advice

Becta / Grid Club, Internet Proficiency Scheme
On-line activities for Key Stage 2 pupils to teach e-safety.
http://www.gridclub.com/teachers/t_internet_safety.html

Kent Local Authority http://www.clusterweb.org.uk/kcn/e-safety_home.cfm
Additional e-safety materials (posters, guidance etc.)

London Grid for Learning
http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/

Grid Club http://www.gridclub.com/teachers/t_internet_safety.html

Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Websites

South West Grid for Learning – Safe www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

South West Grid for Learning – Filtering
http://www.swgfl.org.uk/services/default.asp?page=filtering

Think U Know www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Web-based Resources - for Parents

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International http://www.childnet-int.org/
“Know It All” CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

Derry Hill Primary School 13
17. Notes on the Legal Framework
This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice)
(Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.
A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others.
Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.
Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for
Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.
In order to defend claims that it has breached either the 2000 Regulations or the Human Rights
Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.

Cyber-stalking & Harassment (http://wiredsafety.org/gb/stalking/index.html)
Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to 7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

Alfriston Primary School Pupil ICT Acceptable Use Policy

Alfriston Primary School provides a range of ICT resources which are available to pupils. In order to ensure the safety of pupils when using this equipment, it is important that they abide by the following rules. Failure to comply may result in suspension of access to equipment, or disciplinary action.

Terms of Acceptable Use:

1. Use of Computer systems

Use of any computer purchased or maintained by Alfriston Primary School or accessing any digital system as provided by the school, including but not limited to: the school web site, VLE and email facilities signifies your acceptance of this policy.

2. School Email

Every class from year 1 onwards is provided with an email address, which they can use to send email to other pupils and teachers. No external email facilities are provided for pupils. The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- All email within the school is monitored; email accounts can be checked to ensure compliance with the above rules.

3. Internet Access

The school provides internet access for all pupils in order to allow access to the wide range of content available.

The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasion it may be possible to view a website which is inappropriate for use in a school. In which case the website should be reported to the class teacher.

The use of online real-time chat rooms is banned, unless specific permission is given by the class teacher.

The use of personal online email accounts, such as Hotmail, is banned, the only email facilities to be used by pupils are those provided by the school.

4. Personal use of Equipment

The ICT provisions provided by the school are provided for school work only.
Only activities which have been assigned by the class teacher are permitted.
The only exception to the above rule is the use of E-learning laptops at home.
These may be used for any purpose, subject to the following conditions:

- The usage does not cause any physical damage to the laptop.
- No attempt is made to enter the BIOS of the laptop.
- They are not used for any illegal activities.
- Non-school work is not saved to the thaw drive.

5. Digital cameras

The school encourages the use of digital cameras by pupils, and provides specific cameras for this purpose. Cameras are only to be used under supervision of an adult. Photos and videos captured using the cameras should be appropriate, and not cause offence to anyone.

Under no circumstances should acts of violence or any other infringement of the school's rules be recorded by a pupil.

6. **Security**

Pupils are not permitted to use a computer that is logged on as a member of staff, unless under direct supervision from that member of staff.

7. **File Storage**

Each pupil has their own area on the network which should be used to store all of their work. All work stored should be appropriate for viewing in a school.
The storage of music files, other than those created in school is not permitted.

Staff Agreement

I have read and fully accept the schools ICT policy.
I am aware that breaches of this policy may result in Disciplinary Action.
I am aware than all use of the computer systems can be monitored for the purposes of ensuring compliance with this policy.

Signed …………………………………………………. Date ………………..

Print name ………………………………………………………………………

Pupil's Agreement

I agree that:

- I will only use the computers for school work and homework
- I will ask permission from a member of staff before using the Internet
- The messages I send will be polite and responsible
- I will not give my home address or telephone number or arrange to meet anyone under any circumstances
- I will report to my teacher immediately any unpleasant material or messages sent to me
- I understand that the school will check computer files and will monitor the Internet sites that I visit
- I will not access other people's files
- I will only use my own username and password
- I will not share my username or password with others

Signed …………………………………… (pupil) Class …………………..

Parent's Agreement

I have read and accept the Schools ICT Acceptable use policy. I have discussed the policy with my child.

Pupils Name …………………………………….. Date…………………….

Signed ……………………………… (parent or carer) Print name ………………….