



St. Saviour's Church, Coalpit Heath.

The Manor C of E Primary School

Policy: Acceptable Use of the Internet

Author: Miss J Owen

Date: July 2010

Approved:

.....
.....

Headteacher
Chair of Governors

CONTENTS

1	Rationale
2	The benefits of the Internet to education
3	Designated person for E-safety policy
4	Authorised Internet access
5	Policy links
6	E-safety: a shared responsibility
7	Safe and secure broadband for learning
8	Responsible use by staff
9	Responsible use by pupils
10	Communication with parents
11	Issues, mis-use and complaints
12	Auditing issues
13	Electronic communications
14	Published content and the school Web site
15	Social networking and personal publishing
16	Managing emerging technology

Appendices

E-safety audit (A)
E-safety and acceptable use agreement – pupil responsibility (B)
E-safety and acceptable use agreement – parent responsibility (C)
E-safety and acceptable use agreement – teacher / staff responsibility (D)
Responsible use of the Internet letter to parents (E)
E-safety rules KS1 (F)
E-safety rules KS2 (G)

1 Rationale

E-safety considers the following technologies: PCs, laptops, webcams, digital video equipment, mobile phones, portable media players, games consoles and personal digital assistants. All persons either using technology or supervising the use of technology are required to abide by this policy. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. This policy addresses the core areas identified through Safeguarding boards of infrastructure, policy and protocols and education and training.

E-safety requirements are applicable during the times whereby the school is opened; this applies to term-time, extended school events, lettings for community use. It is also relevant to residential / off-site events e.g. school trips and visits.

2 The benefits of the Internet to education

- a) The Internet fully supports the school's implementation and delivery of a creative Curriculum to enhance learning opportunities.
- b) It provides access to world-wide educational resources.
- c) It provides opportunities for educational and cultural exchanges between pupils world-wide.
- d) It gives access to experts in many fields.
- e) It provides professional development for staff through access to national developments, educational materials and effective curriculum practice.
- f) It provides a means of collaborating across a range of support services.
- g) Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- h) Internet access will be planned to enrich and extend learning activities.
- i) Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3 Designated Persons for E-safety Policy

The school will appoint an e-Safety co-ordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap. Currently this role is shared between Mrs Hilary Eade (Head Teacher and Child Protection Officer) and Miss Owen (ICT Co-ordinator).

4 Authorised Internet Access

Our school will comply with copyright law. It will also maintain a current record of all staff and pupils who are granted Internet access. All staff must read and sign the 'Acceptable ICT Use Agreement', before using any school ICT resource. Parents will be informed that pupils will be provided with supervised Internet access and will be asked to sign and return a consent form for pupil access.

6 E-Safety – A Shared Responsibility

E-safety depends on effective practice at a number of levels:

- a) Safe and secure broadband for learning, including effective management of content filtering.
- b) Responsible use by staff; made explicit through training and published policy.
- c) Responsible use by pupils; encouraged through education.
- d) Good communication with parents and carers to raise awareness of risks.

7 Safe and Secure Broadband For Learning

Internet access is provided through the South West Grid for Learning. This is a filtered service, which is reviewed regularly. It is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Virus protection is provided by the South Gloucestershire Education IT team and our contract states that this is regularly updated. The technician (South Gloucestershire Education IT team) will also regularly monitor Internet access and bring any issues to the attention of the e-safety co-ordinator, who then takes appropriate action. Senior staff will also ensure that regular checks are made to filtering methods and the school will work with the LA, SWGfL, DfCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

8 Responsible Use By Staff

All staff will be given the 'Acceptable Use Of The Internet Policy' and will have its importance explained. Staff are made aware that Internet traffic can be monitored and traced to the individual user. The e-safety co-ordinator will attend regular training in order to keep up-to-date with the latest recommendations and there will be regular briefings for staff. Staff will receive training on how to carry out Internet searches safely and efficiently and minimise risks. Staff must read and sign the 'Acceptable Use Of The Internet Agreement' (See Appendix D). Staff will also receive training on how best to teach pupils about safe Internet use. At Key Stage 1, access to the Internet will be directly supervised access to specific approved on-line materials. Discretion and professional conduct is essential for all staff, at all times.

9 Responsible Use By Pupils

Rules for Internet access will be posted in all networked rooms and pupils will be informed that Internet use is monitored. Teaching about Internet safety is also mapped in to our curriculum to ensure that pupils have relevant learning experiences. A scheme of work identifies what is taught during each year and will include learning about:

- a) The need to keep their user name and password private and not to share this information with anyone.
- b) What forms of Internet use are acceptable and unacceptable. Pupils will be given clear objectives for Internet use.
- c) The effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- d) How to carry out Internet searches in order to reduce the risk of accessing inappropriate material.
- e) The effective and acceptable use of the Internet for web publishing.
- f) How to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- g) The safe use of Internet to support communications.
- h) What to do if they encounter a problem and this includes how to report abuse for key stage 2 pupils.

[KS2 pupils will also be asked to sign the schools 'E-safety Acceptable Use Agreement' – See Appendix B].

10 Communication With Parents

Parents' attention will be drawn to the Schools 'Acceptable Use Of The Internet' policy in newsletters, the school brochure and on the school Web site. All parents will also be asked to read and sign the schools 'E-safety Acceptable Use Agreement' [Appendix C]. In addition, parents will have the opportunity to attend e-safety workshops and guidance will be given about where to seek further advice related to specific issues.

11 Issues, Mis-use and Complaints

- a) Any e-safety issues are logged and dated and the action taken is also recorded. This includes information about the nature of the incident, who was involved and how it was dealt with. This log is reviewed to identify any trends in issues that may need addressing.
- b) If staff or pupils discover an unsuitable site, it must be reported to the E-safety Coordinator who will immediately report it to SWG to ensure it is filtered out.
- c) Complaints of Internet misuse will be dealt with by a senior member of staff and any complaint about staff misuse must be referred to the HeadTeacher.
- d) Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- e) The schools E-safety rules for both KS1 and KS2 clearly state that pupils are to be taught to keep their passwords secret. Children, staff and parents must not share passwords and individual passwords will be issued to ensure that every user is individually responsible at all times for action taken while their user name is in use.

12 Auditing Issues

The school completes the E-safety audit annually (appendices A) and identifies issues to be addressed. Pupil surveys are also completed in Year 2 and Year 6 and issues are identified and followed up.

Technology Specific Issues

13 Electronic Communications, for example, e-mail and text both sent and received

- a) Pupils may only use approved e-mail accounts on the school system.
- b) Pupils must immediately tell a teacher if they receive offensive e-mail or text and all pupil e-mails will be treated as 'public'.
- c) Pupils must not reveal personal details of themselves or others in any online communication, or arrange to meet anyone.
- d) 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.
- e) The forwarding of chain messages is not permitted.
- f) All must be polite and considerate online and report any issues that are likely to cause offence to others.
- g) Teachers will agree with the class rules for collaborating online.

14 Published content and the school web site

- a) The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- b) The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- c) Written parental permission will be sought in reception and year 3 for images and work by pupils to be published on the school website. Between these years parents can contact the school if they decide to withhold permission. All teaching personnel will be provided with the names of pupils in their class, whose photographs are not to be used in this regard.
- d) Images and work can be published to Merlin spaces that are not accessible to the public.
- e) Photographs that include pupils will be selected carefully.
- f) Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

15 Social networking and personal publishing

- a) Access to open social networking sites will be blocked and pupils will be given access only to those sites that are monitored and approved by South West Grid recommendations; this includes the Merlin online platform.
- b) Tools including message boards, blogs, instant messaging and collaboration tools will be used in this safer, closed environment. Within Merlin children will be taught how to safely communicate and publish content.
- c) All communication will be treated as 'public' and children will be asked to agree and sign a code of conduct before access to these tools is given. Misuse of these tools will lead to the application of sanctions including prohibiting or limiting access.
- d) In Years 5 and 6 Pupils will be encouraged to publish content to their e-portfolio within Merlin and this may be made available for parents. A parent will only be able to see their own child's work.
- e) Newsgroups will be blocked unless a specific use is approved.
- f) Although pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, pupils in Y5/6 will be taught about the potential risks of social networking sites and what information should not be shared on such sites. The purpose of this is to acknowledge (although not condoning) the reality that some children may already have access to social networking sites by this age.

16 Managing emerging technologies

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

Appendix A: E-Safety Audit

This quick self-audit is used to help the senior management team (SMT) assess whether the e-safety basics are in place and enables us to monitor safety.

Has the school an e-Safety Policy that complies with CFE guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Have roles and responsibilities in relation to e-safety been clearly identified?	Y/N
Has e-safety training been provided for both students, staff and parents? How frequently? Has it highlighted any issues?	Y/N
Do all staff sign an ICT Code of Conduct on appointment? Do you have one?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students which have been discussed with them?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCfS requirements for safe and secure access (e.g. SWGfL).	Y/N
Has an ICT security audit has been initiated by SMT, possibly using external expertise?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Has monitoring of internet use taken place with any issues being logged?	Y/N
Has an e-safety log been completed and reviewed to identify and issues which need to be addressed?	Y/N
The self-review framework has been completed this year in order to identify and respond to any issues	Y/N
Relevant pupil surveys have been completed and issues have been identified and addressed through teaching	Y/N

Appendix B
E-safety Acceptable Use Agreement
Pupil Roles and Responsibilities

I know that I should never allow anyone to use my password and that I should keep it and any other personal information private.

Finding information on the internet safely

I know:

- That I will get to use the internet if I use it responsibly
- That being responsible means I should not try to visit unsafe sites or register for things I am not old enough for
- That any protection system does not stop all unsafe content
- What to do if I open something that I don't like
- How to search safely to find the information I want
- That I should be supervised to ensure I am keeping safe
- That any information I put up on the web can be read by anyone
- That I should ask permission to use the work of others and credit them if I do
- That I should not copy others work and claim it as my own

Using technology to contact people

I know:

- How to choose my user name carefully to protect my identity
- How to keep my personal information private
- How to use safety features of web sites
- How to limit access to my information
- That e-mails / messages can be intercepted and forwarded on to anyone
- That I should be careful who I add as friends
- That I need to be polite online and friendly online and think about the language I use (it could be forwarded to my parents or head teacher!)
- How to use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- What to do if I receive an offensive message / e-mail including how to keep evidence
- That people online may not be who they seem

Using technology for buying and selling

I know:

- How to tell the difference between web sites for information and web sites selling things
- How to recognise commercial uses of the Internet e.g. iTunes, mobile phone downloads, shopping
- Not to leave computers logged on with my user name or logged on to sites with personal details entered
- That if an offer looks too good to be true it probably is
- That I should not respond to unsolicited online offers
- That I should not use someone else's identity to buy things online

Signed (KS2 only): _____ **Date:** _____

Appendix C:

E-safety Acceptable Use Agreement - Guide for parents

Monitoring Home Use of the Internet

Parents / carers should:

- Ensure that young people access the Internet in a communal room.
- Ask their children about what sites they are looking at.
- Ensure that family computers are password protected and have robust anti-virus software that is regularly updated.
- Ensure content is appropriately filtered for younger users.

Content – finding and publishing information on the Internet

Parents / carers should:

- Ensure that their children know that they will only get to use the Internet if they use it responsibly and that being responsible means they should not try to visit unsafe sites or register for things they are not old enough for.
- Ensure that their children know that any protection system does not stop all unsafe content and that children need to tell them if they access something inappropriate.
- Encourage children to search safely to find the information they want and search safely themselves using very specific search terms to reduce the likelihood of accessing unsafe material.
- Supervise younger children when they are using the Internet.
- Talk to children about the fact that any information published on the web can be read by anyone.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves in danger.

Contact - Using technology to contact people

Parents / carers should:

- Discuss user names with children and talk about how to choose them carefully to avoid putting themselves at risk and protect their identity.
- Identify the information that young people should keep private in order to prevent them being contacted or traced.
- Talk to children about the need to use safety features of web sites.
- Talk to children about limiting access to their personal information.
- Explain that e-mails / messages can be intercepted and forwarded on to anyone.
- Talk about being careful and about who they should add as friends.
- Talk about the need to be polite and friendly online and think about the language they use (it could be forwarded to other parents or the head teacher!)
- Discuss how to use the subject field in e-mails.
- Explain why not to open messages if the subject field contains anything offensive or if the person it is from is not recognised (delete it without opening it).
- Discuss what to do if an offensive message / e-mail is received, including how to keep evidence.
- Explain that people online may not be who they seem.

I have discussed these issues with my child.

Signed: _____

Date: _____

Appendix D:

E-safety Acceptable Use Agreement - Teacher and Staff Roles and Responsibilities

Finding information on the internet safely

The school should:

- Have clear rules on Internet use displayed in each class and ensure that they have been discussed in class.
- Teach children about safe Internet searching.
- Teach children about protecting passwords and usernames.
- Test searches prior to children using them to ensure that there is less risk of inappropriate results being found.
- Supervise children when they are using the internet.

Using technology to contact people

Teachers should:

- Teach all pupils what information not to disclose over the Internet and how to keep their identity private.
- Treat all communications using school based e-mail etc as 'public', checking that children communicate politely and responsibly.
- Provide a safe, protected space where children can communicate initially only with other children from the school/ region.
- Teach your child about the hazards of social networking.
- Talk to children about the fact that any information published on the web can be read by anyone.
- Teach your child that someone on the internet may not be who they seem.
- Check information that your child is publishing on the web before it is posted to ensure that they are not putting themselves in danger.
- Teach pupils what to do if they get sent inappropriate material or are a victim of cyber-bullying.

Using technology to for buying and selling

Teachers should:

- Teach pupils to identify sites that have a commercial motive.
- Teach pupils to automatically close pop-ups.
- Teach pupils how to avoid basic identity theft or fraud.

Signed: _____

Date: _____

Appendix E:

Dear Parent/ Carer,

As part of your child's curriculum and development of ICT skills, The Manor C of E Primary School is providing supervised access to the Internet. We believe that the use of the Internet is worthwhile and is an essential skill for children as they grow up in the modern world. We expect all pupils to be safe and responsible when using any ICT and we feel that it is essential that pupils are aware of E-safety issues and how to keep themselves safe on-line.

At The Manor C of E Primary School a number of steps have been taken to minimize the risks of E-safety issues arising, including:

- a) Using a filtered Internet Service Provider.
- b) Ensuring children are supervised while using the Internet.
- c) Using safe / child-friendly websites that have been viewed by staff prior to use.
- d) Making regular checks of the computer's Internet browser, bookmarks or history.
- e) Teaching the children the SMART rules and helping them to understand how they can use the Internet safely.

We would appreciate your support in this endeavour and have attached our 'E-safety and Acceptable Use Agreement' for you to discuss with your child. Please sign to say that you have talked about each point with your child and that you are happy to follow the agreement. If you have any concerns regarding your child's Internet use or require further explanation, please discuss them with your child's class teacher or come and speak to me at the end of the school day.

Yours sincerely

Mrs Eade and Miss Owen
Head Teacher and ICT Co-ordinator

Appendix F:

Key Stage 1

These are our rules for using the Internet safely.

Our Internet and E-mail Rules

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using the Internet safely.
- We can go to www.thinkuknow.co.uk for help.

Appendix G:

Key Stage 2

These are our rules for using the Internet safely and responsibly.

Our On-line Rules

- We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail, chat to or video-conference people an adult has approved.
- Adults are aware when we use on-line tools, such as video-conferencing.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips without permission and never include names with photographs.
- If we need help we know who to ask.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we know what to do.
- If we receive a message sent by someone we don't know we know what to do.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using the Internet safely and in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.