Monmouthshire Primary Schools E-Safety Core Policy Guidelines and Audit

January 2009

Produced by Mark Davies Schools ICT Development Manager &
Emma Taylor Healthy Schools Co-ordinator

Primary School Core Policy

This core e-Safety Policy may be used by primary schools as the basis to construct their own policies.

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Acceptable Use Policy has been superseded to reflect recent developments and raise awareness of safety issues associated with electronic communications as a whole.

The Core e-Safety Policy

This core e-safety policy provides the essential minimum e-safety policy that every primary school in Monmouthshire should have.

Page 3 comprises of an e-safety audit that should be carried out annually when reviewing this policy.

Pages 4 to 7 comprise of the template policy which should be amended to fit your school, **no sections should be deleted**. Extra information can be added if a school feels it is appropriate.

Pages 8 to 10 comprise of an exemplar permission form to be sent home to parents. We recommend it gets completed twice during their time in Primary School, once when starting and then again upon entering Year 3.

Page 11 comprises of an exemplar Staff ICT Code of Conduct which should be filled in by all new staff before they are allowed access to ICT in school.

Pages 12 and 13 comprise of Internet Safety posters which should be displayed next to every computer in the school. These are examples for Key Stage 1 and 2 (which should be different), you could of course come up with your own rules and design a poster specifically for your school.

Additional Resources

As well as resources for you to use for teaching e-safety in school, we can provide assemblies on e-safety for Key Stage 2 and also assist in holding parent seminars to empower parents and carers in e-safety, for more information contact Mark Davies.

Further Information

Schools ICT Development Manager / Healthy Schools Co-ordinator

Monmouthshire's e-Safety Resource Pack

E-Safety materials and links as published on www.moned.org.uk

Becta Curriculum e-safety advice

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities.

Has the school got an e-Safety Policy that complies with MCC guidance?	Yes
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The Designated person responsible for Child Protection is: Mr Gorell	
The member of staff responsible for e-safety is:Mrs McCormick & Miss Way	
Has e-safety training been provided for both students and staff?	Yes
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Yes
Have school e-Safety Rules been set for students?	Yes
Are these Rules displayed in next to all computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with MCC requirements for safe and secure access.	Yes
Has an ICT security audit has been initiated by SMT, possibly with the support of MCC or external expertise?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes
Further comments:	

St Mary's RC Primary School

E-safety policy

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing.

The school's e-safety policy will operate in conjunction with other policies including:

- Pupil Behaviour
- Anti-Bullying
- Child Protection
- PSE Policy
- Curriculum

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

• Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

• Safe and secure broadband including the effective management of filtering.

• A member of staff being responsible for the implementation and monitoring of this e-safety policy.

Introduction

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in St. Mary's for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly.

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 personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.

School web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified.
- Pupils' full names are not used anywhere on the Web site or blog.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school Web site *(see Appendix 1 for sample permission form)*.
- Pupil's work will only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school blocks access to social networking sites.
- Newsgroups are also blocked.
- Pupils are told never to give out personal details of any kind which may identify them
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported immediately to the e-Safety Coordinator.
- Senior staff ensures that regular checks are made to ensure that the filtering methods are appropriate and effective.

Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy decisions

Authorising Internet access

- All staff read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource *(see Appendix 2 for sample Staff Agreement)*.
- The school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access is withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the Internet will be by supervised access to specific, approved on-line materials.
- Parents are asked to sign and return a consent form.

Assessing risks

- The school takes all reasonable precautions to ensure that user's access only appropriate material by using Monmouthshire's filtering system.
- The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse is referred to the head teacher.
- Complaints of a child protection nature are dealt with in accordance with the school's child protection procedures.
- Pupils and parents are informed of the complaints procedure.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year *(see Appendix 3 for Internet Safety Rules)*.
- Pupils are informed that network and Internet use will be monitored.
- As part of the National Curriculum and skills development, Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff have copies of the school's e-Safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.

Enlisting parents' support

- Parents' attention is drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school Web site.

This policy will be review annually by the governors and staff or in light of new guidance.
E-safety policy – {Date}

Appendix 1

Dear Parents

As part of our commitment to the education and use of ICT in our school, we are writing to you to give you information on how your child and we as a school use ICT. Please read the following information and rules carefully and sign the appropriate boxes on the form if you wish to give your consent.

Please Note: You do not have to sign all parts, just the ones you give permission for. Just leave the other blank.

1. Internet Access
Your child will have the opportunity to access and use the Internet and a Virtual Learning Environment (VLE) as a learning resource during their 7 years in this school. Our Internet access is monitored, filtered and supervised at all times to avoid pupils accessing unsavoury material. As part of our policy we request that you sign the **box 1** if you want to give your child permission to use the Internet in school.

Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home. You may find it useful to visit web sites such as www.thinkuknow.co.uk – a web site designed by the police with an aim to highlight Internet security and how to stay safe with your child when online. Also, www.getnetwise.org - GetNetWise is a public service brought to you by a wide range of Internet industry corporations and public interest organisations.

2. Publication of work on our web site
There is nothing that children like more than seeing their work on the Internet and showing it to their family. Occasionally we put work on our web site. Please sign box 3 if you give consent to work your child produces being published on our web site.

3. Publication of photographs on our web site
We also ask that you consider giving permission to the use of photographs being published on the school's web site. We are fully aware of the security implications and **do not** put names of children next to a photo. To find out more about our use of images on the web site, visit our web site and click on 'Terms & Conditions'.

Now you have read the above information, think about whether you want to give consent. Please consider that by giving your child consent you are allowing them to have the opportunity to access some excellent resources that will enhance your child's learning throughout their time in school.

There is also a fourth box, which is for your son/daughter to sign. Please read through the rules on the next page with your child and discuss what they mean to ensure they understand what they are signing. Younger children will not be able to understand them; therefore we ask that you sign on their behalf.

For your information, as part of the curriculum your son/daughter will be taught about Internet Safety throughout school.

Should you wish to discuss any aspect of Internet use or view the schools policy on ICT and E-Safety, please telephone us to arrange an appointment.

Yours sincerely

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

St. Mary's RC Primary

Responsible Use of the Internet, VLE, Pupil Work & Photographs

Please complete, sign and return to class teacher

Pupil:	**Class:**

Box 1. Parent's Consent for Internet Access

I have read and understood the school rules for responsible use of the Internet and VLE & and give permission for my son/daughter to access and use it. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.

Box 1 Signed:	**Date:**

Please print name:

Box 2. Parent's Consent for Web Publication of Work

I agree that my son/daughter's work may be published on the VLE and/or web site.

Box 2 Signed:	**Date:**

Please print name:

Box 3. Parent's Consent for Web Publication of Photographs

I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Box 3 Signed:	**Date:**

Please print name:

Pupil Agreement

Box 4. Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Box 4 Signed: by pupil or on behalf of pupil	**Date:**

Appendix 2

Staff ICT Code of Conduct

To ensure that you are fully aware of your professional responsibilities when using ICT in school, you are asked to read and sign this code of conduct. You should consult the school's e-safety policy for further information and clarification.

- The ICT systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my ICT use will always be compatible with my professional role.
- I understand that ICT may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my ICT and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ..... Date: .....

Print Name: .....

Accepted for school: ..... Print Name: .....

Appendix 3

Key Stage 1

These rules help us to stay safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.