Risca Primary School

E- Safety Policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Risca we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Risca Primary School.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's e-safety coordinator is Headteacher/ICT Manager
- The e-safety Policy and its implementation shall be reviewed bi-annually.

Roles and Responsibilities

Headteachers and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher/Senior Leaders are responsible for ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteachers/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteachers /Senior Leaders should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The ICT Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in supporting the Leadership Team to review the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- 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 asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher/ICT Manager, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Email

- E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-safety:
- 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 without specific permission.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a using outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

- Social networking Internet sites (such as, MySpace, Facebook) provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.
- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, family and staff over the Internet and deny access to others.

- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Teachers immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require LT intervention (e.g. cyberbullying) should be reported to LT in the same day.

Allegations involving staff should be reported to the Headteachers. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed. Evidence of incidents must be preserved and retained. The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a

safety/precautionary use. These are handed into the school office at 8:45 and collected at the end of the day.

- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom/one of the school offices.

On trips staff mobiles are used for emergency only

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- To secure good safeguarding procedures for our pupils, parents and carers are not permitted to take photos/videos of their own, or other pupils in school events. School will take approved photographs and place then on the school Twitter feed.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- One of the Headteachers/ICT Manager or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of

Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to one of the Headteachers.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as msn. This will be strongly reinforced

across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School e-safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School e-safety Policy in newsletters and on the school Website.

Further Resources

We have found these web sites useful for e-safety advice and information.

http://www.thinkuknow.co.uk/	Set up by the Police with lots of information for parents and staff including a place to report abuse.
http://www.childnet-int.org/	Non-profit organisation working with others to "help make the Internet a great and safe place for children".

Acceptable Use Agreement/Code of Conduct: Pupils

Risca Primary School Student Internet Publishing

Statement of Purpose

Risca Primary School is pleased to offer our student's access to the World Wide Web and other electronic networks. The advantages afforded by the rich, digital resources available today through the Internet outweigh any disadvantage. However, it is

important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved. Internet safety is also an important concern.

When enrolling in Risca Primary School, every parent grants permission to allow their child to access the Internet at school following the guidelines of the Caerphilly County Borough Council, Education Department User Access Policy. In recent times, Internet-based resources have become more interactive, allowing students to publish work, visible to a wider, often global audience through resources such as a classroom blog or wiki.

Online communication is critical to our students' learning of 21st Century Skills and tools such as blogging, podcasting and video production offer an authentic, real-world vehicle for student expression. Publishing student pictures and work on websites promotes learning, collaboration and provides an opportunity to share the achievements of students. Images and products of students would only be included on school websites without identifying captions or names. Again, as educators, our primary responsibility to students is their safety. Hence, expectations for classroom blog, student protected e-mail, podcast projects or other Web interactive use must follow all established Internet safety guidelines.

Internet Safety

- Parents and Users. Despite the best efforts of supervision and internet filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
- Personal Safety. In using the network and Internet, users should not reveal personal information such as home address or telephone number. Users should never arrange a face-to-face meeting with someone "met" on the Internet without a parent's permission.
- Confidentiality of Student Information. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
- Active Restriction Measures. Caerphilly Education Department utilises filtering software and other technologies to prevent students from accessing websites that are (1) obscene, (2) pornographic, (3) harmful to minors and; (4) Anti-social, or promote illegal activity. The use of anonymous proxies to bypass content filters is strictly prohibited and will be considered a violation of the acceptable use policy. The school also monitors the online activities of students, through direct observation and/or technological means.

Student Use of New Web Tools Blogging/Podcasting Terms and Conditions:

- The use of blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes but is not limited to profanity; racist, sexist or discriminatory remarks.

- Students contributing to the class blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their content. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers).
- Comments made on class blogs must be moderated by the teacher and - if deemed inappropriate – deleted.
- Links to external web sites from the class blog or from a blog comment are to be checked to verify they are appropriate for a school setting.

Students who do not abide by these terms and conditions may lose their opportunity to take part in the class blog project and lose internet access privileges as specified in the School Discipline Policy.

School Responsibilities

- Will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the school curriculum.
- Use of networked resources will be in support of educational goals.
- Treat student infractions of the Acceptable Use Policy according to the school discipline policy.
- Provide alternate arrangements for students who do not have access to use the internet at home..

TERMS AND CONDITIONS

Pupils wishing to access the World Wide Web facilities provided on the network must agree to act in a considerate and responsible manner as defined in this contract. The ICT Technician may review files and communications to maintain the system and ensure that pupils are using the network responsibly. Pupils should not expect that files stored on school servers will always be private.

INAPPROPRIATE BEHAVIOUR DEFINED

- Accessing, displaying offensive messages or pictures or other inappropriate material. Should pupils encounter such material by accident, they must report it to a member of staff immediately.
- Accessing Internet chat rooms, newsgroups, games or materials not pertaining to work needs
- Subscription to any services or ordering of any goods over the Internet.
- Accessing E-mail through services NOT provided by the school without prior permission. This includes services such as HOTMAIL, FREESERVE, YAHOO etc.
- Downloading or installing any software (shareware/freeware or software demos) onto school network drives or local computers.
- Violating copyright laws by copying, saving or redistributing copyrighted material. This includes any other illegal activity.
- Using other's passwords or accounts, even if another person allows it.
- Trespassing in others folders, work, files or vandalising the data of another user.
- Intentionally wasting limited resources by printing materials not related to school work.

Access
Parental or guardian permission is required. The use of the network is a privilege, not a right, and should be treated as such. to network services is given to pupils who agree to act in a considerate and responsible manner.

Any action taken by a pupil which is a violation of this contract will be subject denial of Internet facilities and/or network privileges. Your signature(s) on the attached agreement is/are legally binding and indicate that the terms and conditions of the agreement have been fully understood by all parties who have signed. If there is something that you do not understand, please contact the ICT Technician/Manager at Risca Primary School on 01495 244566 for advice.

Parents, please retain the terms and conditions (this page) for your records. The attached agreement must be signed and returned to school to permit your daughter's/son's in-school use of the Internet and other network resources.

PUPIL AND PARENTAL CONTRACT

This contract replaces any previous agreement and will remain valid until your child leaves Risca Primary.

DATE: _____

PUPIL'S FULL NAME: _____

YEAR GROUP: _____

PARENT OR GUARDIAN:

As the parent or guardian of this pupil I have read and agreed to the Terms and conditions of the Acceptable Use Policy. I understand that this access is designed for educational purposes and the pupil named above is expected to use the resources according to the specified guidelines. I have discussed these guidelines with my daughter/son and believe that he/she understands them. I also recognise that Risca Primary has done everything in its power to protect pupils from inappropriate information available on the Internet and I will not hold Risca Primary responsible for materials my daughter/son may acquire on the network.

I hereby give my permission for the pupil named above to use the Internet at Risca Primary and certify that the information contained in this form is correct.

I understand that a copy of this agreement will be kept on file at Risca Primary.

Name of PARENT/GUARDIAN: _____

RELATIONSHIP TO PUPIL: _____

SIGNATURE: _____

From time to time, RISCA PRIMARY photographs may be displayed on the school's website. If you object to your daughter's/son's picture being displayed in this way, please tick this box. ☐

PUPIL:
I have read the Acceptable Use Policy and will abide by these rules. Having discussed it with my Parent(s)/Guardian(s), I understand why the Internet is available at Risca Primary and also understand that I must follow these rules when I use the computers. I know that if I do not follow the rules, I may not be permitted to use the Network and/or the Internet and disciplinary action and/or appropriate legal action may be taken.

PUPIL'S FULL NAME: _____

SIGNATURE: _____

Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log By the e-safety coordinator/ICT Manager.

This Incident log will be monitored termly by the e-safety co-ordinator/ICT Manager and Headteacher.