Brynteg County Primary School

e-Safety Policy

Writing and reviewing the e-safety policy

The school has appointed an e-Safety coordinator. This is the Headteacher, Designated Child Protection Coordinator as the roles may overlap.

Our e-Safety Policy has been written by the school, building on the Wrexham e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why the Internet and digital communications are 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 high-quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

Internet use will enhance and extend learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

School ICT system security will be reviewed regularly.

Virus protection will be installed and updated regularly.

Security strategies will be discussed with ICT Learning and Teaching Advisory Service and WCBC IS Department.

E-mail

Pupils may only use WCBC approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Messages sent using the schools email system should not be considered private and the school reserves the right to monitor all email.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The school should consider how e-mail from pupils to external bodies is presented and controlled.

The forwarding of chain letters is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

The headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing pupils’ images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.

Pupils’ full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

Wrexham IS department will, by default, block / filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

Members of staff will not engage in dialogue about the school or with parents through the use of social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils should not place personal photos on any social network space without considering how the photo could be used now or in the future.

Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing filtering

The school will work in partnership with WCBC IS Department and the ICT Learning & Teaching Advisory Service to ensure that systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the web site address and a description of the inappropriateness of its content must be reported to the schools e-Safety Coordinator and the person responsible for monitoring filtering.

If staff or pupils come across on-line material which is believed to be illegal (e.g. child pornography), the computer will be quarantined – its power removed and physically secured from tampering. Details will be reported immediately to the E-Safety coordinator and head teacher and Wrexham IS department notified. Outside agencies such as the Police will be informed as appropriate.

The filtering service provided by the IS Department protects staff and pupil computers from viruses and intrusive material, e.g. spy-ware. To further protect staff and pupil computers a suitable anti virus product which is kept up-to-date is installed on all computers used for Internet access.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

If a web site or part of a web site is blocked by the Internet security systems which the school believes staff and/or pupils should have access to, details of the web site and a description of why access is requested will be passed to the designated person in school responsible for reviewing the schools filtering policy.

The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by ICT advisers and Wrexham IS department.

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.

The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

The appropriate use of Learning Platforms will be monitored and reviewed.

Mobile phones will not be used during lessons or formal school time.

The use by pupils of mobile phones, cameras and music players will be kept under review.

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Staff will be issued with a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

All pupils will sign the school's "E-Safety Rules" consent form.

Parents/carers will be asked to sign and return a consent form.

Any person not directly employed by the school will be asked to sign and agree to 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. 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 computer connected to the school network. Neither the school nor WCBC can accept liability for any 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 and effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse will be referred to the headteacher.

Pupils and parents will be informed of the complaints procedure (see schools complaints policy).

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communicating e-Safety

Introducing the e-safety policy to pupils

e-Safety rules will be posted in all rooms where computers are used.

Pupils will be informed that network and Internet use will be monitored.

A programme of training in e-Safety will be developed, including guidance from CEOP, WISE Kids and Becta.

Staff and the e-Safety policy

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

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Staff should understand that phone or online communications, including use of social networking sites, with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

The school will maintain a list of e-safety resources for parents/carers.

Equal Opportunities

The governors and staff are committed to providing the full range of opportunities for all pupils, regardless of gender, disability, ethnicity, social, cultural or religious background. All pupils have access to the curriculum, and the right to a learning environment, which dispels ignorance, prejudice or stereotyping.

Declaration

This policy was approved by the School's Governing Body on ………………………
Signed …………………………….Chair of governors.
It will be reviewed during the Summer Term of 2018

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation	
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on 'moderated sites' and by the school administrator.	Making the News Headline History National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News Museum sites, etc. Digital Storytelling BBC – Primary Art National Education Network Gallery
Communicating ideas within chat rooms or online forums.	Only chat rooms created within the Moodle or other Learning Platforms dedicated to educational use and that are moderated should be used. These must only be accessible to pupils and staff within the school. Access to other social networking sites	Moodle

	should be blocked. Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils’ work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	Moodle National Archives “On-Line” Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

Wise Kids
http://www.wisekids.org.uk

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Consent Form

Gaining pupils' and parents' agreement to the e-Safety Rules is important but will require management. Many schools obtain this at the same time as checking the home and emergency contact details once each year.

To ensure clarity, the e-Safety Rules appropriate to the age of the pupil should be included with the letter to parents.

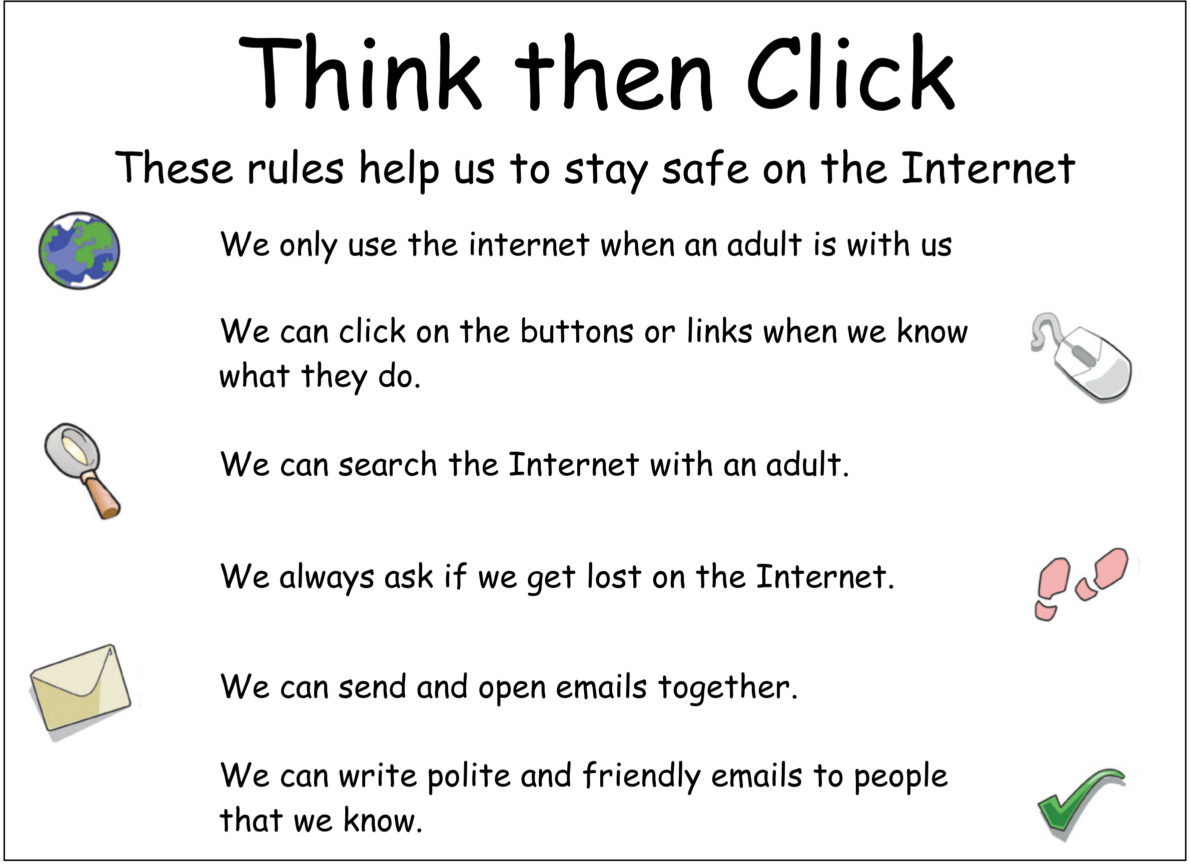
It is important to start from the assumption that ICT and Internet use is everyday and essential for every child's education. The agreement between parents and the school could include a phrase such as:

> ***All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.***

For pupils above the age of 16 and not living at home and for all pupils 18 or older, the school may decide to rely on the consent of the pupil alone. Otherwise parent's consent must be obtained. It is also wise to obtain parent's permission to publish pupil's work. Permission to publish is required for pupil images, video and audio on a Web site, a podcast or video programme.

Where schools arranged purchase, rent or lease portable computers for use by pupils at home, a more comprehensive agreement is required.

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.

Our School
e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: ***Form:***

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.

Signed: ***Date:***

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published. 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.

Parent's Consent for Internet Access
I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school office

These rules apply at all times, in and out of school hours whilst using school equipment and accessing school's Information Systems. Internet, e-mail and access to a Virtual Learning Environment (VLE) will be provided for you to carry out research, communicate with others and access your learning resources on the understanding that you agree to follow these rules. At all times you should use e-Learning resources in an appropriate and responsible manner.

You should:

☑ Be aware that your actions on the Internet, when using e-mail and in the VLE can be seen and monitored.

☑ Always keep your username and password private and secure. *If you feel someone may know your password change it or ask your teacher to help you change it.*

☑ Be aware that information on an Internet web site may be inaccurate or biased. Try to verify the information through other sources before using it.

☑ Take care not to reveal personal information through email, personal publishing, blogs or messaging.

☑ Never arrange to meet strangers who you have met through the Web or e-mail; anyone can pretend to be someone else.

☑ Treat others as they would expect to be treated and write messages carefully and politely, particularly as email could be forwarded to unintended readers.

☑ Always tell your teacher or another adult if you ever see, hear or read anything which makes you feel uncomfortable while using the Internet, e-mail or VLE.

☑ Respect copyright and intellectual property rights. *You cannot use the words or pictures that you see on an Internet site without permission or giving credit to the person that produced the information originally. You must not copy text or pictures from the Internet and hand it in to your teacher as your own work.*

☑ Check with a teacher before: downloading files; completing questionnaires or subscriptions forms; opening e-mail attachments.

You should not:

✘ Send, access, store or display offensive messages or pictures.

✘ Use any chat or social networking forums e.g. MSN , MySpace, Bebo, IM etc

✘ Connect an external device like a USB drive, phone or any other removable media to a computer. *A teacher or the network manager will assist if you have work that needs to be transferred.*

✘ Use or send bad, threatening or annoying language nor use any language which might incite hatred against any individual or ethnic and religious group.

✘ Access any other user's files, e-mail or personal web space without their express permission.

Please note:

The school owns the computer network and can set rules for its use. It is a criminal offence to use a computer or network for a purpose not permitted by the school. The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Our School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil: ***Form:***

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.

Signed: ***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. 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.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: ***Date:***

Please print name:

Please complete, sign and return to the school office

Staff Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using Information Systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarity.

Use of ICT systems:

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not leave laptop computers or any other easily transportable ICT equipment unattended at any time.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that e-mail should not be considered a private medium of communication and that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any software or hardware without permission.
- I will not introduce floppy disks, CDs, memory sticks or any other device into the system without first having checked them for viruses.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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 the schools e-Safety policy and agree to follow the schools code of conduct.

Full name: …………………………………….………………………… **Date:** ……………………………

Signed: ……………………………………………………………

Accepted for School: ……………………………………............ **Date:** ……………………………