Ysgol Cefn Mawr

E-Safety Policy

Learning Enjoying Achieving

1. Writing and Reviewing the e-Safety Policy

- The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- The school has appointed an e-Safety Coordinator (Mr Simon Williams) who will work closely alongside the Child Protection Coordinator (Mrs Ceren Williams)
- 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 and the PTA.
- The e-Safety Policy and its implementation will be reviewed annually.

2. Teaching and learning

2.1 The Importance of Internet and Digital Communications

- The internet is an essential element in 21st century life for education, business and social interaction. Ysgol Cefn Mawr recognises its 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.

2.3 Internet Use to Enhance Learning

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.
- PC Erin Hulley (School Liaison Officer) holds annual Internet Safety workshops with Years 2, 4 and 6, normally to coincide with Safety Internet Day.
- To strengthen the message about the importance of internet safety the school holds a poster competition for Internet Safety Day.

2.4 Evaluating Internet Content

- At Ysgol Cefn Mawr we ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught the importance of questioning internet materials before accepting its accuracy.
- Pupils are taught how to report unpleasant internet content.

3. Managing Internet Access

3.1 Information System Security

- Our school ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

3.2 E-mail

- Messages sent by the school email system are not considered to be private and the school reserves the right to monitor all email.
- Pupils may only use WCBC approved e-mail accounts on the school system.
- Whole-class or group e-mail addresses will be used in most situations.
- Pupils are aware that they 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. Pupils are made aware of email policy and reminded regularly.
- Incoming e-mail from unknown sources are treated as suspicious and attachments are not opened unless the author is known.
- When e-mail is sent from pupils to external bodies it will be sent via the teacher's email account and checked thoroughly before it is sent. This ensures the teacher can read/check any response to make sure it is suitable, before pupils see the content.
- The forwarding of chain letters is not permitted.

3.3 Published Content and the School Website

- The contact details on the School Website is of the school office.
- Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for our website and ensures that content is accurate and appropriate.

3.4 Publishing Pupils Images and Work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. When possible we use group photographs rather than full-face photos of individual children.
- 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 is obtained before photographs of pupils are published on the school Web site.
- Work is only published with the permission of the pupil and parents/carers.

- Pupil image file names will not refer to the pupil by name.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

3.5 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.
- Ideally pupils would use only moderated social networking sites outside of school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites outside of school.

3.6 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 Wrexham IS department Help Desk by the person responsible for monitoring filtering in the school.
- 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.

3.7 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.
- Mobile phones will not be allowed in school unless specific permission has been given by the Headteacher. They will not be allowed on during lesson time.
- Games machines including the Sony Playstation, Microsoft Xbox and others that have Internet access which may not include filtering are not allowed in school.
- Staff are not allowed to take photographs of the children with their personal mobile phones i.e. when out on field trips.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

3.8 Protecting Personal Data

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

4. Policy Decisions

4.1 Authorising Internet Access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- In the Foundation Phase access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Pupils will be asked to sign the school's "E-Safety Rules" consent form along with their parents or carers.
- 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.

4.2 Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor WCBC can accept liability for the material accessed, or any consequences of Internet access.
- At Cefn Mawr we will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

4.3 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.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- 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.
- Discussions will be held with the Police School Liaison Officer to establish procedures for handling potentially illegal issues.

4.4 Community Use of the Internet

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

5. Communications Policy

5.1 Introducing the e-Safety Policy to Pupils

- E-Surfers promise will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, including guidance from CEOP, WISE Kids and Becta.
- E-Safety training will be embedded within the ICT scheme of work.
- Mr Simon Williams is the E-Surfer coordinator.
- There are 6 pupil E-Surfers.
- The E-Surfers complete challenges every term and they teach every class.
- E-Surfers conduct assemblies about e-safety.
- E-Surfers have produced their own code of conduct.

5.2 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 will always use a child friendly safe search engine when accessing the web with pupils.

5.3 Enlisting Parents' Support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

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	Only chat rooms created within the	Moodle

within chat rooms or online forums.	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 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)

This policy was reviewed by Simon Williams and adopted by the Finance/Staffing Committee on 8 November 2022.

Signed _____ Head Teacher

Signed _____ Chair of Finance/Staffing Committee

Review date: June 2023

Appendix 2: Useful Resources for Teachers

Google Internet Legends including wellbeing lesson plan and Interland
https://beinternetlegends.withgoogle.com/en_uk/toolkit

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/Carers

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

Good Websites
Kid rex, duck duck go, google safe search

Bad Websites
Google, Bing, Yahoo, Wikipaedia.

Ysgol Cefn Mawr

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:	***Class:***

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

Ysgol Cefn Mawr
E-surfers
Code of Conduct

1. Always use a safe search engine
e.g. kuddle, kidrex, google safe search.

2.Never be rude online.

3.Tell a parent, teacher or e-surfer if you have been cyber bullied.

4.Ask permission before using the internet.

Ysgol Cefn Mawr e- surfers

October 2019

Appendix 5

YSGOL CEFN MAWR
E-Surfer Logo