e-Safety Policy

Signed:

Date:

Review Date:

Our overall ambition in all we do is to ensure our pupils have excellent opportunities to develop into:

- ambitious, capable learners, ready to learn throughout their lives
- enterprising, creative contributors, ready to play a full part in life and work
- ethical, informed citizens of Wales and the world
- healthy, confident individuals, ready to lead fulfilling lives as valued members of society.

This e-safety policy has been approved by the WCBC ICT Strategy Group and adopted by our school.
WCBC considers that the policy elements with a **W** bullet are mandatory in order to protect staff, pupils, the school and WCBC.
Bulleted items are optional. These have been added selectively where the school feels that aspect of e-safety is appropriate.

Our overall ambition in all we do is to ensure our pupils have excellent opportunities to develop into:

- ambitious, capable learners, ready to learn throughout their lives
- enterprising, creative contributors, ready to play a full part in life and work
- ethical, informed citizens of Wales and the world
- healthy, confident individuals, ready to lead fulfilling lives as valued members of society.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and students;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband;
- A school network that is compliant with National Education Network standards and specifications.

Writing and Reviewing the E-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, anti-bullying and for child protection.

- **W** The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- **W** The 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.
- **W** The e-Safety Policy and its implementation will be reviewed regularly.

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 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.

Internet use will enhance learning

- **W** The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- **W** 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 will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

- **W** The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

- **W** School ICT systems security will be reviewed regularly.
- **W** Virus protection will be updated regularly.
- **W** Security strategies will be discussed with the Local Authority.

E-mail

- **W** Messages sent using the schools email system should not be considered private and the school reserves the right to monitor all email.
- **W** Pupils may only use WCBC approved e-mail accounts on the school system.
- **W** Whole-class or group e-mail addresses will be used in most situations.
- **W** Pupils must immediately tell a teacher if they receive offensive e-mail.
- **W** In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- 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

- **W** 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 content is accurate and appropriate.

Publishing pupil's images and work

- **W** Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.
- **W** Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- **W** Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or other learning platforms.
- **W** Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- **W** Wrexham IS department will, by default, block / filter access to social networking sites.
- **W** Newsgroups will be blocked unless a specific use is approved.
- **W** Members of staff will not engage in dialogue about the school or with parents through the use of social networking sites.
- **W** Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- 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.

Managing filtering

- **W** 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.
- **W** 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 (local authority).
- **W** 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.
- **W** 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.

- **W** Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable (Service Level Agreement).
- **W** 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.

Managing videoconferencing & web cameras

- **W** Videoconferencing should use the educational broadband network to ensure guaranteed quality of service and security.
- **W** Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- **W** Any faults with Videoconferencing equipment should be reported to the IS Department Helpdesk who will assign an appropriate technician to resolve any faults.
- **W** Videoconferencing and web camera use will be appropriately supervised for the pupils' age.

Managing emerging technologies

- **W** Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- **W** The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Mobile phones will not be used during lessons or anytime when in contact with children.
- 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 e.g.Chums / Friends.
- Smart watches are not permitted in school.
- Staff should not use personal mobile phones to photograph pupils.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- **W**All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource (Appendix 1).
- **W** The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- **W** In the foundation phase access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- **W** 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.

Assessing risks

- **W** 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.
- **W** The school will audit ICT use in line with our monitoring to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- **W** Complaints of Internet misuse will be dealt with by a senior member of staff.
- **W** Any complaint about staff misuse will be referred to the headteacher.
- **W** Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- **W** Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- **W** Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

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

Communications Policy

Introducing the e-safety policy to pupils

- **W** E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly (Appendix 4 and 5).
- **W** Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- **W** 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 or the Personal Social and Health Education (PSHE) curriculum.
- Digital Leaders are in place in school and use child net to help keep pupils safe.

Staff and the e-Safety policy

- **W**All staff will be provided with a copy of the School e-Safety Policy for their perusal and its importance explained.
- **W** Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- **W** 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 safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- **W** Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- **W** The school will maintain a list of e-safety resources for parents/carers.
- **W** The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school (Appendix 3).

Appendices

1. Staff Code of Conduct
2. Parental Consent for web publication for work and photographs
3. Parental / Pupil Agreement
4. E-Safety Rules Foundation Phase
5. E-Safety Rules

Appendix 1
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, unless I am using it in the place it resides e.g. hall.
- 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.

Only encrypted memory sticks will be used to store personal / school data.

- 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 students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will respect my professional role when using social networking sites, ensuring I don't publish comments / photographs which could bring my professional position into question.
- I will not publish photographs of children without parental permission or other staff members without their consent.
- 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:** ……

Appendix 2

Parent's Consent for Web Publication of Work and Photographs

I agree that my child's work may be electronically published. I also agree that appropriate images and video that include my child 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 child to use electronic mail and access the Internet. I understand that pupils will be held accountable for their own actions. I will be informed of any inappropriate use. 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 accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

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

Appendix 3
e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the Foundation Phase /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's Name:
D.O.B:

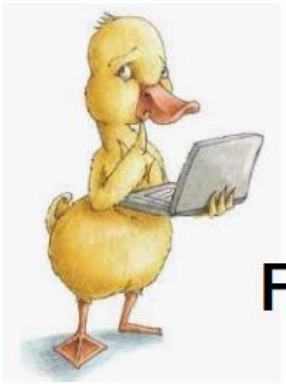
I understand the school e-Safety Rules.

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:

Appendix 4
e-Safety Rules Foundation Phase



E-SAFETY RULES

For Foundation Phase

Never share any things about yourself.

If you feel sad or scared tell an adult.

Make sure that a grown up you trust says that you can go online.

Never give out any passwords.

Remember not everyone is who they say they are.

Do not agree to meet up with someone you meet online.

Do not say or do anything that will hurt or upset others.

Think carefully about what you post online.

Appendix 5
e-Safety Rules

E-SAFETY RULES

Never give out any personal information to strangers.

Talk to a trusted adult if you feel uncomfortable about anything.

If someone asks you to meet up with them tell them no and tell a trusted adult.

Make sure you have adults permission before going online.

Think about others feelings when messaging or chatting to other people online.

Keep your privacy settings as high as possible.

Remember your digital footprint- everything you post online stays there forever even if you delete it.