Ysgol Rhosnesni

E-Safety Policy

V4

Date Reviewed	**January 2022**
V4	**Annually**

RHS e-safety policy

The e-Safety Policy is part of the RHS School Development Plan and relates to other policies including those for ICT, Bullying and for Child Protection. It has been written by the school; building on the WCBC eSafety Policy and government guidance.

It has been written and agreed by the school's Head of ICT, Senior Leadership Team and approved by Governors. The Policy and its implementation will be reviewed annually.

The designated Child Protection Co-ordinator will also be the e-Safety Co-ordinator.

This document can be viewed at www.rhosnesni-high.wrexham.sch.uk. A paper copy may be requested from the main school office.

1 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 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.

1.1 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.

1.2 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2 Managing Internet Access

2.1 Information system security

- The 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.

2.2 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 school's e-mail 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 will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online will be the school office and the attendance officer.
- The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

2.4 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- As part of the admission process, written permission from parents or carers will be obtained before photographs of pupils are published on the school web and social media sites.
- Work can only be published with the permission of the pupil and parents/carers.

2.5 Social networking and personal publishing sites

Parents and teachers should be aware that the internet has emerging on-line spaces and social networks which allow individuals to publish unmediated content. e.g. Snapchat, Instagram

Writing for an audience is important to language development and an essential life skill. However, students should be encouraged to be cautious about revealing too much personal information and about the difficulty of removing inappropriate text, images or other content once it is published.
Some potential dangers of such technologies include:

- Providers that do not supply any solid ownership or contact information for their sites
- The dangers inherent when sites can be set up using a false name and e-mail address with no identity checking
- The posting of anonymous comments that may be malicious
- Sites that give safety of users a low priority
- Sites that celebrate inappropriate and unacceptable behaviour

In response the School will:

- Filter access within school in line with the published policy on 'Acceptable use of Electronic Communications'
- Be proactive in educating students so that they have a good understanding of what it means to be a responsible and mature user of internet technologies
- Explain to students the risks and how to get help should they need it
- Discourage students from posting personal information about themselves and each other
- Teach students to critically evaluate materials and learn good searching skills
- Provide opportunities within a range of curriculum areas to teach about e-Safety
- Provide parents and the school community with information relating to the safe use of computers and offer constructive advice on how to minimise risk to their children
- Deal with any incidents relating to e-Safety via the Behaviour Policy

2.6 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 school's 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 co-ordinator and Headteacher 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 school's 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.

2.7 Managing videoconferencing & web cameras

- Videoconferencing should use the educational broadband network to ensure guaranteed quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Any faults with Videoconferencing equipment should be reported to the IS Department Helpdesk who will assign an appropriate technician to resolve any faults.
- Video conferences should be booked using the Janet Video Conferencing (JVCS) booking service to ensure that video conferences are not double booked. The JVCS will also transparently facilitate IP to ISDN conferences at no charge to the school.
- Videoconferencing and web camera use will be appropriately supervised for the pupils' age.

2.8 Mobile Device Safety

Mobile phone technology has advanced significantly over the last few years - and it continues to evolve. Wireless connections in particular have extended the capabilities of mobile phones, enabling access to a wide range of new content and services globally. Many phones now offer Internet and email access, alongside the most often standard functions of messaging, camera, video and sound recording.

Mobile phones, alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance; however there are also associated risks. Children and young people used to understand these risks in order to help them develop appropriate strategies for keeping themselves safe. As with e-safety issues generally, risks to children and young people can be broadly categorised under the headings of content, contact and conduct and managed by reducing availability, restricting access and increasing resilience.

We promote safe and appropriate practice through establishing clear and robust acceptable use guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools - which in turn can contribute to safeguarding practice and protection.

The school rules for the use of mobile phones states:

> If a student brings their phone into school, we insist that the device is switched off and concealed safely in their bag whilst in the school grounds and buildings. Headphones must not be worn or be visible on the school site. Under no circumstances may mobile phones be used at break or lunchtimes. If mobile phones/headphones are seen in school, staff will confiscate them from students to be collected at the end of the school day (main reception). Students who persistently fail to comply with this rule will receive further sanctions.

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of indecent images, exploitation and bullying. It is also recognised that mobile phones can cause an unnecessary distraction during the working day and can be intrusive when used in the company of others. When mobiles phones are misused it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

Mobile safety is promoted through PSE, the house system and during Safety week.

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.

2.9 Protecting personal data

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with GDPR 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. For further information please see the School Privacy notice and associated Policy.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

In order to comply with statutory legislation and to support and enhance your child's education and wellbeing we share your child's personal information with a number of establishments, organisations and third party companies. Everyone we share your data with has a data sharing agreement in place with the school; this ensures your data is safe and secure whilst in their possession and will only be used for the purposes in which they are engaged. Please visit the school website for further information.

3 Policy Decisions

3.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. This will be signed as part of the school's new starter process and the form will be provided and stored securely by the Network Manager.
- 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.
- 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.

3.2 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 RHS 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.

3.3 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.
- Pupils and parents will be informed of the complaints procedure (see Complaints Policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

- Complaints of a child protection nature will 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.

3.4 Community use of the Internet

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

4 Communicating e-Safety

4.1 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.
- A programme delivered to all year groups when focussing on ‘Safer Internet Day’.

4.2 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 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.

4.3 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 maintain a list of e-safety resources for parents/carers.

4.4 Parental Consent

Once admission has been agreed to Ysgol Rhosnesni, all parents/carers will be requested to complete an online consent form that asks for parental consent to/for:

- Committing to working with the school to ensure that the e-safety rules have been understood and agreed.
- Consent for internet access.
- Consent for the transferring and processing of data via Hwb.
- Consent for Web publication of work and photographs.
- Consent for routine off site visits.
- Consent for the sharing of data through third party agreements (as per Appendix 1 of the school’s Fair Processing Privacy Notice).
- Specific consent for use of the school’s biometric cashless system.

This parental consent when received, is recorded on the student’s school record.

e-safety for pupils with additional needs

e-Safety for Pupils with Additional Needs

Possible ways to support a generic group of children who may require additional support to move forward in safeguarding themselves.

A fundamental part of teaching e-safety is to check pupils' understanding and knowledge of general personal safety issues.

Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, Internet use.

Rules are very helpful to all pupils and it is important to achieve consistency of how rules can be applied.

- This is a difficult area for some pupils who will usually learn rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers. The school will consider whether a scheme or resources are applicable or accessible to all school situations where Internet access may be possible.
- As consistency is so important for these pupils, there is a need to establish e-safety rules for school that are similar to those for home. Working with parents and sharing information with them would be relevant to all children, but this group especially.
- There will always be exceptions to rules and if this is the case, then these pupils will need to have additional explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the Internet.
- It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of *what might happen if*… without frightening pupils.

How rules are presented could be vital to help these pupils understand and apply some of the rules they need to learn.

- Visual support is usually important to help most pupils' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.
  - Uncomfortable
  - Smart
  - Stranger
  - Friend

  It might be helpful to ask pupils to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms.
- Visual support can be useful but it is more likely that the pupils will respond to multi-media presentations of the rules such as interactive power-point slides, screensavers, spoken recordings of the main rules or sounds that they can associate with decisions they make while using the Internet. The really useful thing about these is the repetition and practice that pupils can have with these which may not be so easy if spoken language were used.
- If visual prompts are used to help remember the rules, the picture or image support needs to give the pupils some improved understanding of what the rule is about. It is quite easy to find attractive pictures that link to other abstract ideas not related to Internet use i.e. use of a

compass to show “lose track” of a search when a head looking confused is more like what happens.

- This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the Internet individually, but also when with peers.

    - It can be common for peers to set up scenarios or “accidents” regarding what they look for on the Internet and then say it was someone else who has done so. Adults need to plan group interactions carefully when raising awareness of Internet safety.
    - Some pupils in this group may choose recreational Internet activities that are perhaps simpler or aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. Staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with Internet use.

- For various reasons, pupils with additional needs may find it difficult to explain or describe events when using the Internet

    - Some pupils might find it easier to show adults what they did i.e. replay which will obviously have it’s own issues for staff regarding repeating access
    - Some pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions.

- Some may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.

    - Pupils may need a system or a help sound set up on computers which will help them to get adult attention. If pupils don’t recognise that they need help, then adult supervision is the safe way to improve their recognition of this.

Useful websites for resources

www.gridclub.com

www.kidsmart.org.uk

www.thinkuknow.co.uk

www.netsmartz.org

www.bizzikid.co.uk

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

e-Safety and use of the Ysgol Rhosnesni High School Computer Network:

The Internet is an essential element in 21st century life for education, business and social interaction. Ysgol Rhosnesni 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 pupils.

Although Internet use is supervised in school and we have taken steps to block access to inappropriate material, you need to be aware that some pupils may find ways to access material which is inaccurate, defamatory, illegal or potentially offensive to some people.

We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages.

During school, teachers will guide pupils towards appropriate material. Outside school, parents/carers bear the same responsibility for guidance as they exercise with other information sources such as telephones, films and radio. Parents/carers have a role for setting and conveying the standards that their children should follow when using media and information sources.

A full version of the RHS e-Safety Policy document can be viewed on the School website. A paper copy may be requested from the main school office.

The e-Safety and Network Rules below should be kept for future reference.

e-Safety Rules for students

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 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
- 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 use of the Ysgol Rhosnesni network must be in support of education and research and consistent with the educational objectives of the school.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- The use of the Internet is a privilege, not a right and inappropriate use will result in the loss of this privilege.
- A log of all Internet access and activity is monitored by the school.
- If an Internet resource could be construed to be of a questionable nature, the burden of responsibility lies with the pupil to check with a member of staff that the resource is suitable.
- The school may deny access to the Internet if a pupil is found abusing privileges.
- Vandalism will result in cancellation of privileges and the appropriate school sanction.
- The school monitors the use of its computer systems, including access to web-sites, the interception of e-mail. Inappropriate materials will be deleted where it believes unauthorised use of the school's computer system has taken place or if it has been used to store unauthorised or unlawful text, imagery or sound.

Student Agreement - Acceptable Use document for use of Hwb

- Remember, anything you do on Hwb should have an educational purpose. You should not regard any of your activity as private or confidential.
- Be a positive role model in how you use digital technologies including Hwb.
- Keep your username and password safe. You are responsible for anything that happens under your account.
- Report to your Hwb administrator if you suspect that your username and password have been compromised.
- If you share external links within Hwb then you deem that the content of the external website is age appropriate and has an educational purpose, e.g. YouTube.
- You may not access, distribute or place material on Hwb that is in breach of the statutory rights of copyright owners.
- Protect the school community by reporting anything you see that might cause upset or harm to yourself, other teachers or learners in the school. You are expected to demonstrate a professional approach and respect for learners and their families and for colleagues and the school while online.
- Creation or transmission of any offensive, obscene or indecent images, data or other material is prohibited. Content relating to or supporting illegal activities may be reported to the authorities.
- Personal use of your mailbox and cloud storage is to be avoided. E-mails may be monitored.
- Comply with the terms and conditions for use of Hwb.
- Always keep another local copy of your essential work that you store on the cloud.

Note: Unacceptable use (as highlighted but not limited to that above) may result in action being taken.

Please note:

- The use of the RHS network must be in support of education and research and consistent with the educational objectives of the school.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- The use of the Internet is a privilege, not a right and inappropriate use will result in the loss of this privilege.
- A log of all Internet access and activity is monitored by the school.
- If an Internet resource could be construed to be of a questionable nature, **the burden of responsibility** lies with the pupil to check with a member of staff that the resource is suitable.
- The school may deny access to the Internet if a pupil is found abusing privileges.
- Vandalism will result in cancellation of privileges and the appropriate school sanction.
- The school monitors the use of its computer systems, including access to web-sites, the interception of e-mail. Inappropriate materials will be deleted where it believes unauthorised use of the school's computer system has taken place or if it has been used to store unauthorised or unlawful text, imagery or sound.

I have read the school's e-Safety policy and agree to follow the school's code of conduct.

Full name: …………………………………………………………………..

Date: ……………………………

Signed: ……………………………………………………………

This form will be kept securely by the School Network manager