YSGOL Y GOGARTH

Nant-y-Gamar Road
Craig y Don
Llandudno
Conwy
LL30 1YE

T: 01492 860077

E-SAFETY POLICY

Teaching and learning

Internet is an essential part of 21st century life and has a valuable role to play in the education of our pupils. Our school has a duty to provide our pupils with quality internet access as part of their learning experience. As a school we recognise that e-safety encompasses internet technologies and electronic communications, such as mobile phones as well as collaboration tools and personal publishing, which is why we have an e-Policy rather than an Internet Safety Policy. We also recognise that e-safety highlights the need to educate pupils about the benefits and risks of using technology as well as our responsibility to provide safeguards. We need to make all users aware of e-safety and help them to control their online experience.

All teachers using ICT in the classroom have a duty to ensure that pupils are reminded about appropriate behaviour regularly. Our school is aware that some of the information on the internet is inappropriate for our pupils and that we need to have an e-safety policy which is understood by and adhered to by all members of staff. This policy defines the appropriate and acceptable use of the internet by both staff and pupils.

- **Why is Internet use important?**
  The rapid developments in electronic communications are having many effects on society. Home and social Internet use is expanding and it is becoming an important part of learning and communication during leisure time.

- **How does Internet use benefit education?**
  The use of the Internet is part of the Digital and Competency Framework (DCF) in Wales. The use of the internet is embedded across the 4 strands of the DCF; Citizenship, Interacting and Collaborating, Producing, Data and Computational thinking. We believe that the internet is a valuable teaching resource that can enhance learning and raise educational standards by offering pupils and teachers opportunities to search for, and access multimedia information from a range of sources all over the world. We understand that as with any school resource ICT needs to be managed carefully to ensure its educational effectiveness and safe usage.

- **How can internet use enhance learning**
  Access to life-long learning and employment both require computer and communications use and pupils need to develop ICT life skills. Whilst we are a ‘Special School our pupils use the Internet and ICT on a daily basis and we believe that their e-safety education should begin as soon as technologies are introduced.

- **How will pupils learn how to evaluate Internet content?**
  Pupils will use age-appropriate tools to research Internet content. This brings pupils into contact with a wider range of information, the scope and nature of which may, or may not, be appropriate for the pupil. There are also wider dangers that social media platforms could all be used as a means of anonymous communication with pupils by adults with inappropriate intentions. See policy on Social media.

Managing information systems

The school’s ICT systems capacity and security is managed by Conwy ICT department. The ICT technician will ensure that virus protection is updated regularly and take responsibility for Firewall and antivirus software. The provision of Broadband internet access is organised and managed by Conwy Council’s ICT Services Department.

- **How will information systems security be maintained?**
  - the security of the school information systems and users will be reviewed regularly
  - virus protection will be updated regularly
  - unapproved software will not be allowed in work areas or attached to email

  - files held on the school’s network will be regularly checked
  - Conwy ICT Department will review system capacity regularly
  - the use of user logins and passwords to access the school network will be enforced

- **How will email be managed?**
  Where appropriate, pupils can have access to HWB an online learning platform where they can have their own email accounts. All staff have access to their own school email account and Hwb email account.

  - pupils may only use approved email accounts for school purposes
  - pupils must immediately tell a designated member of staff if they receive offensive email
  - pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
  - whole-class or group email addresses will be used throughout the school for communication outside of the school
  - staff will only use official school provided email accounts and seesaw to communicate with pupils and parents/carers, as approved by the Head teacher.
  - excessive social email use can interfere with learning and will be restricted
  - the forwarding of chain messages is not permitted
  - staff should not use personal email accounts for sending sensitive school information
  - the official school email service may be regarded as safe and secure and is logged
  - users need to be aware that email communications may be monitored
  - users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
  - any digital communication between staff and pupils or parents/carers must be professional in tone and content
  - personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
  - the school ICT provider ensures mail is virus checked (ingoing and outgoing), includes spam filtering and backs emails up daily

- **How will published content be managed?**
  The point of contact on the Website is the school address, Headteacher’s e-mail address and the school telephone number. Staff or pupils’ home information will not be published. We want our school web site to reflect the diversity of activities, individuals and education that takes place at Ysgol Y Gogarth. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be.

- **Can pupils’ images or work be published?**
  Photographs of children can only be published to the website with the parents’ written permission. (Records of which parents have given consent can be found in the class registers). Pupils’ full names will not be used anywhere on the website, particularly associated with photographs.

- **How will filtering be managed?**
  Pupils have limited access on the internet under their login. Staff logins give more access but it is still rigidly filtered.

- **How are emerging technologies managed?**
  Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- **How should personal data be protected?**
  In order to protect data subjects’ personal information, data protection law (as amended by GDPR) requires all data controllers to follow these key principles:-

  - Fair, lawful, and transparent processing

- Purpose limitation
- Data minimisation
- Accuracy
- Data retention periods
- Data security
- Accountability

(Please see data protection policy for further information)

Policy decisions

- **How will Internet access be authorised?**
  All staff will read and sign the Staff Acceptable Use Agreement before using any school ICT resources. Parents will be asked to read and sign the School Acceptable Use Agreement for pupil access and discuss it with their child, where appropriate.

- **How will risks be assessed?**
  The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences resulting from Internet use. 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. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.

- **How will the school respond to any incidents of concern?**
  All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content, any signs of radicalisation or extremism etc). The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log. The Designated Senior Person for Safeguarding will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

- **How will e–Safety complaints be handled?**
  All e–Safety complaints and incidents will be recorded by the school, including any actions taken. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with the school to resolve issues. All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- **How will Cyberbullying be managed?**
  Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- **How will Learning Platforms be managed?**
  The Senior Leadership Team and staff will regularly monitor the usage of the learning platform by pupils and staff in all areas, in particular message and communication tools and publishing facilities. Pupils/staff will be advised about acceptable conduct and use when using the learning platform.

- **How will mobile phones and personal devices be managed?**
  Mobile phones and other personal devices such as Games Consoles, Tablets etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly. Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, social media platforms, camera phones and internet accesses all common features. However, mobile phones can present a number of problems when not used appropriately:-

- they are valuable items which may be stolen or damaged
- their use can render pupils or staff subject to cyberbullying
- Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering
- they can undermine classroom discipline as they can be used on “silent” mode
- mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff

Mobile phones and personal devices will not be used during lessons or formal school time. PLEASE SEE SEPARATE MOBILE PHONE POLICY. They should be switched off at all times. Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Staff Use of Personal Devices

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy then disciplinary action may be taken.

All staff will be given the school e-safety policy and the importance of the policy will be clearly explained. The e-safety policy will be available on the school website for both teachers and parents to access. All staff should be aware that Internet traffic can be monitored by the Internet Administrator and can be traced to the individual user. Discretion and professional conduct is essential.

Parents will be given a copy of the School e-safety Policy. We have also created a page to support parents in using ICT at home with their children safely. We hope that taking an active role in providing parents with information and guidance about e-safety we will further protect our pupils and help to ensure that they are getting e-safety messages in the home too. We realise that parents and carers have a key role in promoting e-safety at home. ICT offers the opportunity for children and parents to learn together and e-safety is a topic which can be taught at home and school.

Who will write and review the policy?

The ICT Subject Leader takes responsibility for managing e-safety within our school working in conjunction with the designated Child Protection Coordinator and the Internet Administrator. The e-safety policy and its implementation will be reviewed annually and the school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Appendix 1

STAFF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USE AGREEMENT

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are asked to read and sign this Acceptable Use Agreement.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, tablets, digital cameras, email and social media sites

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system)

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018 and UK GPDR

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, tablets, mobile phones). I will protect the devices in my care from unapproved access or theft

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information

- I will respect copyright and intellectual property rights

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

- I will report all incidents of concern regarding children’s online safety to the Designated Child Protection Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or if I have lost any school related documents or files, then I will report this to the ICT Support Team

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address, seesaw app or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership Team

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the Law

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School’s Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service’s information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ………………………….... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….

Eco-Schools

iNet
International Networking for Educational Transformation

Welsh Network of Healthy School Schemes
Cynlluniau Ysgolion Iach - Rhwydwaith Cymru

ACTIVE
MARC
2010-13 CYMRU

BRITISH COUNCIL
INTERNATIONAL
SCHOOL AWARD
2012–2015

Living the Olympic
and Paralympic Values

Marc Gyrfa Cymru
Careers Wales Mark

AUTISM
ACCREDITATION