Polisi E-ddiogelwch
E-Safety Policy

Ysgol Tryfan

Llofnodwyd ar ran Cadeirydd y Llywodraethwyr:
Signed on behalf of the Chair of Governors:

Dyddiad Cymeradwyo: **Mawrth 2024**
Date of Approval:

Dyddiad Adolygu: **Mawrth 2027**
Review Date:

1. Introduction

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

1.2 Our e-Safety Policy has been agreed by senior management and approved by the governors.

2. Learning and teaching

2.1 The Internet and digital communications are important because:

- The Internet is a vital element in 21st century life for education, business and social interaction.
- The school has a duty to deliver good quality access to the internet as part of their learning experience of Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet use will benefit education because it:

- Gives access to educational resources from around the world
- Enables collaboration across support services and professional associations
- The exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government

2.3 Internet use will improve pupils' learning because:

- The internet access at the school is designed specifically for pupil's use and will include filtering appropriate to the age of pupils
- The pupils are learning from what Internet use is acceptable and what is unacceptable and given clear objectives for using internet
- Pupils will be taught to use the Internet effectively in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be taught how to publish and present information to a wider audience.

2.4 Pupils will learn how to evaluate Internet content:

- To ensure that school of materials used by Internet staff and pupils complies with copyright law
- For pupils from learning about the importance of checking information before accept that it is correct
- For pupils to learn how to report any objectionable content e.g. how to use the CEOP Report Abuse icon

3. Management Information Systems

3.1 Safety information systems

- School ICT systems are reviewed regularly
- The system of protection against viruses is regularly updated and security strategies discussed with the Local Authority

3.2 Email

- Pupils can use approved e-mail accounts on the school system
- Pupils must tell a teacher / teacher immediately if they receive offensive e-mail
- In relation to communications via email, pupils must not reveal their personal details or any other details, or arrange to meet anyone without specific permission
- Sending chain letters are not allowed
- Be suspicious of incoming emails and do not open until identifying who the author is
- Schools should consider how emails from pupils to external bodies are monitored

3.3 Published content and the school website

- Contact information for staff or pupils will not be published

- On-line contact details should be kept in the school office
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupil's images and work

- Photographs that include pupils will be carefully selected in order to ensure that individuals cannot be identified and images cannot be misused. can not be identified or their image misused.
- We will consider using group photographs rather than photos of individual photos of children.
- Pupils' full names will not be used anywhere on the school's website or any other website, especially with photographs.
- Permission must be sought from parents or carers before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents / carers.
- Children's full names will not be used on the website, especially with photographs.
- Parents should understand the school's photographing and publishing policy, how they are stored at school and on independent electronic equipment.

3.5 Protection of personal data

- Personal data is recorded, processed, transferred and made available in accordance with the Data Protection Act 1998.

4. What does electronic communication include?

- Internet collaboration tools: social networking sites and web logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones and tablets, computers with internet communications: e-mail and instant messaging
- Webcams and videoconferencing
- Wireless games consoles

4.1 Social networking and personal publishing

- Social Network sites and newsgroups will be filtered unless specific use is approved
- Pupils will be advised not to introduce any sort of details that could mean someone can identify them, their friends or their location
- Ideally, pupils would use only moderated social networking sites, eg SuperClubs Plus
- Students and parents will be advised that the use of social network spaces outside school a range of dangers for pupils
- Pupils will be advised to use nicknames and avatars in the use of social networking sites

5. In exceptional circumstances it may be necessary to use live streaming technology. This technology allows a member of staff to teach a group of pupils without being in the same place as them. The teacher and pupils can be in their homes e.g.

5.1 Safeguarding learners and their wellbeing is paramount, both take precedence over all other considerations when planning live streaming lessons.

- Always follow your school's safeguarding policies. All online security issues should be dealt with in the same way as you would for an face-to-face learning issue.
- If you have any safeguarding concerns about a child, you should discuss them with the Designated Person responsible for Child Protection.

5.2 Before streaming live lessons the purpose, benefits and limitations of a live streaming lesson should be considered:

- Consideration should be given to whether another method is more suitable, e.g. if the teacher intends to show how to do something, a video may be more appropriate.
- Think about which learners will be available, e.g. will all learners be available at the same time, will some need to join or leave at different times? It is recommended to consider the number of learners on a session

5.3 Make sure that the length of live-streamed lessons is suitable for your learners.

5.4 The lesson should be planned in advance, and learners and parents / carers should be given sufficient notice. This will also contribute to how safe the session will be.

- Ensure all content is appropriate, and for any tasks that involve researching online, make sure the websites are suitable before the lesson.

- All learners should have access to necessary software programs.

- If the lesson involves tasks, remember that some learners may need more time.

5.5 Permission should be obtained from the senior management team to stream live lessons informing them of the timetable for each lesson. A live streaming lesson should not be run without the knowledge of the senior management team.

5.6 It should be ensured that appropriate usage agreements are in place for all learners involved in a live-streamed lesson. The agreement will set out the clear expectations of all parties, and set out the steps that will be taken if the agreement is not complied with.

5.7 Professional conduct

Any live streaming work should take place on a voluntary basis, and education practitioners who choose live streaming should continue to work in a professional manner as they would in the classroom. Teachers should do the following:

- Adhere to professional standards of dress when in front of the camera.
- Not have one-to-one live-streamed lessons with learners.
- Be aware that comments are being heard by many learners in an online environment, and that it would be easy to misinterpret comments.
- Make sure they end the session for everyone, making sure learners are not left alone and unsupervised in a session after the teacher has left.
- Be aware of the need for confidentiality; especially if you are streaming a lesson live from a location where other adults or children are present.

5.8 Recording live streaming sessions

A recording facility is available on Microsoft Teams and Google Meet**. All live learning sessions must be recorded.**

Because live streaming recording is synonymous with personal data, you must comply with your school's data protection policies and GDPR regulations

5.9 Learners' behaviour

When working with children and young people, you should make clear at the beginning of each session what is expected and what behaviour is acceptable.

Education practitioners should do the following:

- Make it clear that 'classroom standard' behaviour is expected of all present.
- Set expectations from the start.
- Create and agree clear ground rules and standards of behaviour, based on the school's current behaviour management policy.
- Explain the rules when presenting the lesson, e.g. who can speak, how to ask a question or ask for help. If this is the first time that lessons have been held online, it may take a while to get used to the new environment. By using the chat function, it will be possible to engage in a structured way with those present.
- Continue to remind learners of the rules agreed at the start of each lesson (Appendix 2), and explain how they can raise concerns if necessary.

6. Management filter

- If staff or pupils come across unsuitable material online, the site must be reported to the eSafety coordinator
- Senior staff will ensure that regular checks are completed in order to ensure that the filtering methods selected are appropriate, effective and reasonable

7. Managing emerging technologies

- Emerging technologies will be of educational benefit and they are examined for risk assessment before being used at the school
- The senior management team should note that technologies such as mobile phones that access wireless internet may go beyond the school's filtering systems and can present a new route to undesirable material and communications that may be dangerous
- Mobile phones may not be used during lessons or formal school time
- Texting an offensive or inappropriate files via Bluetooth or any other way is prohibited.

8. Policy Decisions

8.1 Internet Access Authorization

- The school will maintain a record all staff and pupils who are granted access to the school's IT systems
- Internet access is permitted only by adult demonstration with direct supervision and by looking at specific online materials that are approved
- Parents will be required to sign and return a consent form
- Any person that is not employed by the school will be required to sign acceptable use of the school's IT policy before accessing the internet from the school site

8.2 Assessing risks

- The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and internet content, it is not possible to guarantee that unsuitable material will not appear on the computer connected to the school network
- The school can not accept liability for any materials found on any computer or any consequences of internet access
- The school should audit IT use to establish whether the e-safety policy is adequate and that the e-safety policy is being implemented in an appropriate and effective manner

8.3 Staff Responsibilities

- Any member of staff that does not comply with the school's policy and uses email or the Internet for inappropriate use is liable to be disciplined
- Staff who manage filtering systems or monitor the use of IT have a great responsibility, and must be properly supervised. The procedures define how to bring improper use or illegal use of IT to the attention of senior management.

- Staff must be aware of the risks to themselves in managing the use of IT, such as viewing inappropriate images to investigate their origin, and to ensure that appropriate security measures are in place to protect themselves
- Any allegation of inappropriate behavior must be brough to the attention of senior management and appropriate steps followed following receiving such information.

8.4 Community use of the internet

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

9. Tackling e-safety complaints

- Senior staff will address complaints in relation to Internet misuse
- Any concerns regarding staff should be directed to the Head
- Child protection complaints will be dealt with in accordance with the school's child protection procedures
- Pupils and parents are aware of the complaints procedure
- Pupils and parents will be told what will happen to pupils misusing the Internet
- Discussions will be held with a Community Police Officer to establish procedures for tackling potentially illegal issues.

9.1 How do we respond?

The Designated Person Child Protection can provide guidance if you are concerned about how the child, young person or staff member's use of the Internet.

9.2 Response to an Incident of Concern

- Internet technologies and electronic communications provide an opportunity for children and young people to broaden their learning experiences and develop the ability to be creative at school and outside school. Nevertheless, it is important to remember the risks associated with using such technologies.
- Recognise and seek to develop skills needed for children and young people in communicating and using these technologies appropriately, whilst keeping them safe, and show respect for others.
- The risks of e-safety are caused by people acting inappropriately or even illegally
- We need to deal with any issues that may arise on a personal level.
- Teachers are the front line of defense; their observation of behavior of pupils is crucial in detecting dangers to pupils and in developing trust so that issues are addressed
- Events will range from mischief or unconsidered action to illegal incidents that are carefully planned
- This section will help staff to determine what action to take and when to report an incident of concern to the person with responsibility for Child Protection or e-Safety within the school
- Following consultation with the designated child protection person, issues can then be referred to the Authority's Child Safeguarding Officer or to the Police if deemed necessary

10. Communication Policy

10.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all rooms where computers are used and discussed with pupils regularly
- Pupils will know that the use of the network and Internet will be monitored in an appropriate manner
- An E-learning training program will be developed
- E-safety training will be included in the work plan of IT and / or curriculum PSE (PSE).

10.2 Staff and the e-safety policy

- All staff will receive the School e-Safety Policy and the importance of the policy will be explained
- Staff must be aware that it can monitor and track the network and Internet traffic to the individual user
- Staff that manage filtering systems or monitor IT use will be supervised by the senior management team working with procedures for reporting issues
- Staff will use a search engine that is safe for children at all times when on the internet with pupils

10.3 Introducing Policy to parents and carers

- Parents and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website
- The school will cascade a list of e-safety resources for parents / carers
- The school will ask parents to sign the parent / pupil agreement when registering children at school

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety matters
Web directories created to provide access to suitable websites.	There should be parental consent. Pupils should be supervised. Pupils should be referred to specific materials that have been approved on-line.
Use search engines to gain information for numerous sites.	The filtration system must be active and be checked frequently. There should be parental consent. Pupils should be supervised. Pupils should learn what Internet use is acceptable and what they should do if they encounter material they are uncomfortable with.
Exchange information with other pupils and ask bloggers and experts questions (via email).	Pupils should use e-mail accounts or blogs approved. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.
Pupils work published on the school website or on other websites	Parental and pupil's consent should be sought prior to publishing any material. Pupil's full names and any other personal details should be removed. Pupil's work should only be published on 'moderated sites' only.
Pupils work published on the school website or on other websites	Parents consent should be sought prior to publishing photographs. Pupils should not be able to be identified from photographs. File names should not refer to the pupils by name. Staff must ensure that the images published is not breaking any copyright laws.
Communicating ideas in chat rooms or online forums	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites will be prevented. Pupils should never give out personal information.
Audio conferencing and video conferencing to gather and share pupils' work.	Pupils should be supervised. Schools should use the programs managed by local authorities and approved Educational Suppliers only.

Appendix 2: Useful resources for teachers and parents

Canolfan Camfanteisio ar Blant a'u Hmddiffyn Ar-lein (CEOP)
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/
South West Grid for Learning
http://swgfl.org.uk/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Internet Safety Zone
www.internetsafetyzone.com
School Beat
https://www.schoolbeat.org/cy/
Parth e-ddiogelwch HWB
http://hwb.wales.gov.uk/esafety-index