

Baglan Primary School



E Safety Policy

Spring 2018; Adopted 12.03.18

Chair of Governors: Mr L Rees

Headteacher: Mrs N E Morgan

Review Date: Spring 2021

E safety training for parents	
27.11.14	PC Ian Wozencroft: School Liaison Officer
11.09.15	PC Ian Wozencroft: School Liaison Officer
12.11.15	BT/ UNICEF Workshop for pupils and parents; Year 5
09.09.16	PC Ian Wozencroft: School Liaison Officer
08.09.17	PC Ian Wozencroft: School Liaison Officer

Baglan Primary School Ysgol Gynradd Y Baglan



Policy for E Safety

Aim:

The purpose of internet use at Baglan Primary School is to raise standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. In addition, we recognise the internet is an essential element in the 21st century for education, business and social interaction. E Safety encompasses the use of new technologies, internet and electronic communication such as: mobile phones, collaboration tools and personal publishing. Our school has a duty to provide students with safe, quality internet access as part of their learning experience.

Writing and reviewing the e safety policy

The e safety policy will operate in conjunction with other policies including:

- Safeguarding/ child protection policy
- Pupil discipline including anti bullying policy
- PSE Policy
- Curriculum Policy
- Data Protection Policy

The school has appointed two e safety coordinators: Mrs E Challenger and Mr C Atkins

Our e safety policy has been written by the e learning manager (Mr Atkins) our e safety coordinator (Mrs E Challenger/ Mr Atkins) and the Headteacher.

It has been agreed by the senior management team and approved by governors.

- The e safety policy was revised by: Mr C Atkins
- It was approved by the governors on: Spring 2018
- The next review date is: Spring 2021

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

- **Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies and clear guidance.**
- **Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.**
- **To teach the children to use the internet safely under supervision, developing their skills and understanding in order for them to manage their own risk as they use the internet independently.**
- **Safe and secure broadband including the effective management of filtering.**
- **A member of staff being responsible for the implementation and monitoring of this e-safety policy.**
- **All staff to be involved in the implementation and management of e-safety, being vigilant to both their use of technology and the monitoring of pupils use in the context to their safeguarding responsibilities.**

The purpose of this policy is to:

- **Through consultation with pupils establish the ground rules we have in Baglan Primary School for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.**
- **Describe how these fit into the wider context of our discipline and PSE policies.**
- **Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.**
- **Understand that accessing inappropriate sites accidentally should be reported to staff immediately.**

TEACHING AND LEARNING

Why the Internet and digital communication 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 part of the statutory curriculum and a necessary tool for staff and pupils.**

- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- The school Internet access is designed expressly for teacher reference and pupil use and includes filtering appropriate to the age of the pupils.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- HWB is a learning platform for educators and learners to share resources, knowledge and experience across the whole of Wales.
- The children are taught the benefits of mobile technologies and how to use them safely.
- The school endeavours to create a consistent message with parents for all pupils and this in turn should aid the establishment and the future development of the school's e-Safety rules.

How does Internet use benefit education?

The benefits of using the internet in education include:

- Access to worldwide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils worldwide
- Collaboration across support services and professional associations
- Exchange of curriculum and administration data with the Local Authority and the Welsh Assembly Government
- Access to learning wherever and whenever convenient
- Access to HWB and Office 365

MANAGING INTERNET ACCESS

How will Information System Security be maintained?

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority
- The school will work closely with the LA to ensure the safety and integrity of any wireless system used or installed in the school
- School or LA data should not be stored on personal devices
- Pupils are not permitted to bring mobile phones to school

- Secure login using WG platform HWB to personal to staff

How will e mail be managed?

- Pupils may only use approved e mail accounts on the school system
- Pupils must immediately tell a teacher if they receive an offensive e mail
- Pupils must not send offensive or inappropriate emails
- In e mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission
- E mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper
- Incoming e mail should be treated as suspicious and attachment not opened unless the author is known
- Whole-class or group e mail addresses should be used in primary schools
- Access to external personal e mail accounts may be blocked
- Account specific to logged in user

How will published content and the school web site be managed?

- The contact details on the school website should be the school address, email and telephone number. Staff and pupils' personal contact information will not be published
- The Headteacher will take overall editorial responsibility and ensure the content is accurate and appropriate

Can pupil's images or work be published?

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using groups photographs rather than full-faced photos of individual children
- Pupils' full names will not be used anywhere on a school web site or other online space, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site

How will social networking and personally publishing be managed?

- Social Network sites and newsgroups will be filtered unless a specific use is approved

- Pupils will be advised never to give out their personal details of any kind which may identify them, their friends or 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
- Children are discouraged from using social networking sites that are not age appropriate
- Chat rooms are blocked
- Pupils must not attempt to gain access to another person/ pupil account
- Pupils are taught not to share passwords with other people

Cyber Bullying: (a form of bullying through the use of ICT)

An effective whole school approach to the prevention of cyber bullying should include:

- An agreed whole school understanding of cyber bullying
- Talking about cyber bullying
- Encouraging children to report any incidents of cyber bullying
- Promoting the positive use of technology
- Regularly monitoring the impact of this policy and the teaching and learning of ICT

Responding to the incident of cyber bullying should be dealt with using the existing behaviour and bullying prevention policies and procedures.

If cyber bullying takes place outside of school and has a negative impact on the orderly running of the school and/or might pose a threat to another pupil during school time or to a member of staff then the Headteacher may take reasonable steps to mediate between the parties.

How will filtering be managed?

- If staff or pupils come across unsuitable online materials, the site must be reported immediately to the e safety coordinator
- The school will work with the LLAN ICT sub group to ensure systems to protect pupils are reviewed and improved

How will video conferencing be managed?

- Video conferencing should use the educational broadband network to ensure quality of service and security
- Pupils must ask permission from the supervising teacher before making or answering a video conference call

- Video conferencing and webcam use will be appropriately supervised for the pupils' age

How can emerging technologies be managed?

- Emerging technologies including Apps for iPad/ iPod will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. This is the responsibility of the e learner manager.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable materials and communication
- Mobile phones are not permitted to be used during the school day. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden
- Apps that enable out of school hours communication between staff and parents (SeeSaw) are able to be monitored by other members of staff within the school and all username and passwords are stored securely. Pupil to pupil interaction out of school hours on apps used by school is not available.

How should personal data be protected?

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

POLICY DECISIONS

How will Internet access be authorised?

- All staff must read and sign the Acceptable Use Policy 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
- At Foundation Phase, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials
- At key stage 2, access to the Internet will be by supervised access to online materials
- Parents will be asked to sign and return a consent form

How will risks be assessed?

- The school will take all reasonable precautions to prevent access to inappropriate material by using NPT filtering system. 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 NPTCBC can accept liability for any material accessed, or any consequences of internet access.
- The school should 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

How will e safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaints about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- The schools' complaints policy is available to all parents

COMMUNICATIONS

Introducing the e-safety policy to pupils

- E-safety rules are posted in all classrooms and discussed with the pupils at the start of each year
- As part of the school's e-Safety work all pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff have copies of the school's e-Safety Policy and know its importance.
- Staff are aware of their responsibility to safeguard all pupils in their use of technology in learning.

Working with the Police

- The school works in partnership with the Schools Community Police Office as part of the schools e-Safety work.
- Some forms of cyber bullying behaviour may involve criminal offences and in these cases the school will contact the SCPO in line with the school's bullying prevention policy.

Working with Parents

- Parents' and carers' attention will be drawn to the school e safety policy in newsletters, the school brochure and on the school website

Baglan Primary School ~ E Safety Policy

- 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

Mr C Atkins
E Learning Manager
Spring 2018

Date agreed: 12.03.18

Headteacher: Mrs N E Morgan

Chair of governing body: Mr L Rees

Date for review: Spring 2021