Ysgol Rhys Prichard School

E-Safety Policy

This policy takes account of 'Information and communication technology in the national curriculum for Wales' (2008) and The 'Skills Framework for 3 to 19 year olds in Wales'. It was written during the Spring Term and presented to and discussed with the staff of Ysgol Rhys Prichard School during the Summer Term 2017. The Headteacher and I.C.T coordinator will review the policy annually and, should amendments be necessary, they will be brought to the attention of all staff and the governing body.

1.1 E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as 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.

The previous Acceptable Use Policy has been superseded by the Carmarthenshire Schools' e-Safety Policy Guidance to reflect recent developments and raise awareness of safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-bullying and Curriculum.

1.2 End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Carmarthenshire County Council including the effective management of Censornet filtering.
- National Education Network standards and specifications.

Further Information

- School Improvement Service
- Primary IT Consultant
- IT Helpdesk
- e-Safety materials and links as published on HWB
- Becta Curriculum e-safety advice

2.1 Writing and reviewing the e-safety policy

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

- The school's e-Safety Coordinator at Rhys Prichard Primary School is the ICT co-ordinator. The E-Safety Co-ordinator is also the designated officer for child protection.
- Our e-Safety Policy has been written to reflect the Carmarthenshire e-Safety Guidance.
- The e-Safety Policy and its implementation will be reviewed annually.

2.2 Teaching and learning

2.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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.

2.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 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.

2.2.4 Pupils will be taught how to evaluate Internet content

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

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Carmarthenshire County Council.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Web site or Blog, 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.

2.3.5 Social networking and personal publishing

- The school will block / filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.6 Managing filtering

- The school will work with the Carmarthenshire County Council IT Services to ensure systems to protect pupils are robust and regularly reviewed.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator and logged in the Incident log book.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted in school for pupils. Staff will not use mobile phones during lessons or formal school time.
- Staff will be issued with a school phone where contact with pupils or parents is required and when off school premises with pupils e.g. school trips, residential camps, sporting competitions etc.

2.3.9 Protecting personal data

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

2.3.10 Password Protection

- All users will have responsibility for the security of their username and password.
- Passwords must not be shared with anyone.
- Any unauthorised use or breach of security must be reported immediately to the E-safety co-ordinator.

- Staff should change their passwords every term. They should not be re-used within 6 months and should be significantly different from previous passwords created by the same user.
- Passwords for new users and replacement passwords for existing users will be allocated by the IT Co-ordinator or Technician.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' (Appendix 1) before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted Internet access.
- In the Foundation Phase, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

2.4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor CCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Education & Children's Service and / or Police to establish procedures for handling potentially illegal issues.

2.4.4 Community use of the Internet

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

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be clearly posted where there is computer access and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure / prospectus and on the school Web site.

Schemes of work across the Curriculum

Through the teaching and learning of Literacy, Numeracy and DCF across the Curriculum we will:

- embed literacy and numeracy skills into learning experiences across all subjects and/or areas of learning;
- develop obvious links between subject schemes of work and/or areas of learning in developing progression in pupils' skills;
- ensure that pupils' skills gained in English/Welsh first language and mathematics lessons are re-visited, reinforced, enhanced and developed further in other subjects and/or areas of learning;
- adapt programmes of study when pupils are working significantly below or above expected levels of literacy and numeracy skills;
- plan for the development of pupils' thinking, planning, creative and problem-solving skills.
- plan in the Foundation Phase to provide a good balance between structured activities for direct teaching of reading, writing and mathematical development and active approaches, including play-based learning;
- plan opportunities for pupils to read and write in areas of continuous provision both indoors and outdoors and in role-play areas;
- plan opportunities for pupils to develop their number, measuring, spacial and data handling skills in areas of continuous and enhanced provision both indoors and outdoors;
- create opportunities for pupils to self-evaluate, evaluate the work of their peers and recognise targets/ next steps for improvement;
- and progressively increase the level of challenge in the work.

In order to track the development of Literacy and Numeracy skills we will:

- Track pupil's understanding through 'Incerts' ('Understood')
- Track provision for teaching throughout for each year group ('Taught')
- Track provision of Literacy and Numeracy skills in each subject/ learning area within the short term planning.

This policy was reviewed by the School's I.C.T co-ordinator in agreement with the staff during the Summer Term 2019. This policy was adopted by the Governing Body of Rhys Prichard School on.

Signed: _____ Chair of Governors **Date:** _____

Appendix 1

Rhys Prichard Primary School
Staff Acceptable Use Policy

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this Acceptable Use Policy. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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, understood and agree with the Acceptable Use Policy.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……