**Ysgol Gynradd Yr Eglwys yng Nghymru Rhaeadr Gŵy**



**Rhayader Church in Wales Primary**

**E-Safety and Acceptable Usage Policy 2021**

E-Safety encompasses Internet technologies and electronic communications 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 school’s e-safety policy operates in conjunction with other policies including those for Behaviour, Bullying, Curriculum and Data Protection.

This e-safety policy provides the essential minimal school e-safety policy.

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.

The Senior Leadership Team (SLT) assesses whether the e-safety basics are in place to support a range of activities using the Hwb 360o.

The aim of this policy is to protect pupils and educate them to be responsible when using ICT.

 ∙ The school appointed an e-Safety Coordinator: Mr David Lewis and the ICT governor is

 ∙ The roles of the Designated Child Protection Governor (Angela Davies) and named members of staff (Linda Crocket, David Lewis and Sian Protheroe) will sometimes overlap.

 ∙ Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.

 ∙ The e-Safety Policy and its implementation will be reviewed annually.

**Teaching and learning**

Why is Internet use 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 a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning.

 ∙ The school Internet access is designed expressly for pupil use.

∙ Pupils are taught what type of Internet use is acceptable and what is not. They are given clear objectives for Internet use.

∙ Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation (Information Literacy). Pupils will be taught how to evaluate Internet content.

∙ The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.

∙ Pupils are taught (where appropriate) to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

**Managing Internet Access Information System security**

∙ The school ICT systems, capacity, security and virus protection is the responsibility of the Local Authority

∙ Pupils may only use approved class e-mail accounts on the school system.

∙ Pupils must immediately tell a teacher if they receive an offensive email.

∙ 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 before sending, in the same way as a letter written on school headed paper.

**Published content and the school website / Twitter feed**

∙ The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils’ personal information will not be published.

∙ The ICT Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Cloud-based Storage**

 ∙ Work created using iPads is stored securely online using the cloud storage space, Microsoft OneDrive via the Hwb. Pupils who do not have written permission for digital imagery consent (see below) will not be permitted to upload content containing images of themselves.

∙ Google Classroom to be the preferred choice of digital storage linked to the cloud.

 **Publishing pupil’s images and work.**

∙ Photographs that include pupils will be selected carefully and will comply with digital imagery consent. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Facebook.

∙ A Digital Imagery consent record is kept (and continually updated) to show those pupils who do/do not have digital imagery permission.

∙ Pupil’s work can only be published with the permission of the pupil and parents.

∙ Pupils’ full names will not be used on the website or Twitter feed.

**Social networking and personal publishing**

∙ The school blocks/filters access to social networking sites.

∙ Newsgroups are blocked unless a specific use is approved.

∙ Pupils are taught never to give out personal details of any kind which 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.

* Video Conferencing projects are organised by teaching staff and pupils are supervised at all times during the session. Permission from parents is sought before any pupil becomes involved in video conferencing projects at a local, national and international level. Any work that is produced by pupils and requires an exchange with another organisation will not be dispatched unless permission is granted by parents or guardians.

∙ Hwb+ is used as a safe, secure, online learning environment accessible to all staff and pupils, advocated by the Welsh Government as an all-Wales learning platform. Pupils are made aware that the content which they publish on the learning platform is made public for all members of the school community to see and is monitored regularly by staff.

∙ The school works with the LA to ensure systems to protect pupils are reviewed and improved whereby a firewall (such as the Smoothwall web filter) will be used to filter out any unsuitable websites.

∙ Pupils using websites for research will be advised on recommended sites, such as BBC Education, wikipedia, with emphasis being placed on safe learning platforms within Hwb.

∙ Pupils are able to access video sites. The Welsh Assembly Government recommends that schools should not fire wall such sites but teach pupils how to use the Internet safely. Therefore, they endorse health and safety on the Internet.

This approach is a strand within the ICT New Order.

∙ If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator. Any incidents need to be recorded in the school office in an appropriate folder.

∙ Children will also be taught Health and Safety on the Internet and are advised on how to act if they bring up any hits that make them feel uncomfortable.

**Protecting personal data**

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

 ∙ CEoP / e-safety training is delivered annually to make all staff aware of safe and acceptable use of the Internet. All staff are asked to sign and agree to an ‘Acceptable use of ICT’ policy [Appendix 1] annually.

∙ The school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil’s access be withdrawn.

∙ In Foundation Phase, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved on-line materials (e.g. Purplemash).

∙ At Key Stage 2, access to the Internet is by adult supervision to approved on-line materials.

∙ The school takes 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. Rhayader Church in Wales Primary School cannot accept liability for the material accessed, or any consequences of Internet access.

∙ The school will be using the ‘360 degree safe’ online self-evaluation tool, which will enable us to evaluate our existing position regarding e-safety and target improvement. Handling e-safety complaints

∙ Complaints of Internet misuse are dealt with by a senior member of staff.

 ∙ Any complaint 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.

∙ Pupils and parents will be informed of the complaints procedure. Communications Introducing the e-safety policy to pupils

∙ E-safety rules and posters are displayed around the school and discussed with the pupils at the start of each year. Pupils sign an acceptable user agreement [Appendix 2] to show that they understand the systems in place.

∙ Pupils are informed that network and Internet use is filtered.

∙ All staff have access to the School e-Safety Policy and its importance explained.

 ∙ Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

* Parents’ and carers’ attention is drawn to the School e-Safety Policy via the School prospectus and also on the School Website.

 ∙ Parents are asked to sign a Parent/Carer Acceptable use of ICT agreement [Appendix 3] to show understanding that making critical, derogatory or malicious comments about the school on social networking sites (i.e. Twitter) is unacceptable and may result in legal action.

**Rhayader Church in Wales Primary School**

**Staff Acceptable Use Policy for ICT**

****

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

Members of staff should consult the school’s e-Safety policy for further information and clarification.

 ∙ I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.

∙ I appreciate that ICT includes a wide range of systems, including mobile phones; PDAs; digital cameras; e-mail and social networking and that only ICT only authority owned (School) equipment should be used for school business.

∙ I understand that school information systems may not be used for private purposes without specific permission from the Head Teacher.

∙ I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.

∙ I will respect system security and I will not disclose any password or security information to anyone.

∙ I will not install any software or hardware without permission from the Head Teacher.

∙ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

∙ I will respect copyright and intellectual property rights and adhere to the Data Protection Act 1998.

* I will report any incidents of concern regarding children’s safety to the e-Safety coordinator, the Designated Child Protection Coordinator or Head Teacher.
* I will ensure that electronic communications with pupils including email, instant messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

∙ I will promote e-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school’s information systems and internet access, to intercept email and to delete 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. Breach of the policy will be considered a serious disciplinary matter and will be dealt with in line with the Disciplinary Policy and procedure.

I have read, understood and accepted the Staff Acceptable Use Policy for ICT.

Signed: ……………………………………………… Print Name: ………………………………………

Date: ………………………………… Accepted for School: …………………………………………………….

Print Name: ……….…………………………………..

**Rhayader Church in Wales Primary School**

**Ysgol Gynradd Yr Eglwys yng Nghymru Rhaeadr Gŵy**

****

**KS2 Pupil Acceptable Use Agreement / e-Safety Rules.**

* I will only use ICT in school for school purposes.
* I will only use my class e-mail address or my own school email address when emailing.
* I will only open email attachments from people I know, or who my teacher has approved.
* I will not tell other people my ICT passwords.
* I will only open /delete my own files.
* I will make sure that all ICT content with other children and adults is responsible, sensible and polite.
* I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher and minimise the screen immediately.
* I will not give out my own details such as my name, telephone number or home address.
* I will not arrange to meet someone unless this is part of a school project approved by my teacher and an adult comes with me.
* I will be responsible for my behaviour when using ICT because I know that these rules keep me safe.
* I know that my use of ICT can be checked and that my parent / carer will be contacted if a member of staff is concerned about my e-Safety.

Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ September 20\_\_\_

This agreement will be renewed annually.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Rhayader Church in Wales Primary School**

**Parent / Carer Acceptable Use of ICT Agreement**

****

The use of social networking sites is not an appropriate media to voice or resolve any concerns you and/or other parents/carers may have about the school.

Our school has an ‘open door policy’ in relation to any concerns that you and/or other parents/carers may have about the school.

The school further implements a complaints procedure which is available to parents/carers on request or through our website.

The school has an e safety policy, which it employs in relation to staff, school pupils as well as parents/carers on social networking and cyber bullying issues.

This policy identifies expectations that parents/carers should adhere to. You may view the policy on our website or view the hard copy at the school by appointment.

If you have genuine concerns regarding the school then you are asked to make an appointment with the head teacher (Mrs Linda Crockett) or ICT Leader (Mr David Lewis).

I understand that, as a parent/carer of a pupil in the school, making critical and/or derogatory or malicious comments about the school on social networking sites (i.e. Facebook, Twitter) is unacceptable and may result in legal action.

Signed: ………………………………………………………….. Date: …………………………….

 Child’s name: ………………………………………………….. Year group: …………………