

# **Llanbedr Church in Wales Primary School**

*Ysgol Yr Eglwys yng Nghymru Llanbedr*



## **E-Safety Policy**

**2021-22**

**Headteacher: Mrs L.J.Green    Chair of Governors: Cllr E. Lusted  
Co-ordinator: Mr Gavin John**

**Signed \_\_\_\_\_ Date: \_\_\_\_\_**

## **Llanbedr Church in Wales Primary School E-Safety Policy**

### **Introduction and rationale**

At Llanbedr Church in Wales Primary School we are committed to providing a caring, friendly and safe environment for all of our pupils and staff so that they can achieve their full potential in a relaxed and secure atmosphere. Information and Communication Technology is an integral part of learning to prepare our pupils for today's society. It is therefore important that we equip them with evaluative skills to use the internet safely in and out of school. Acknowledging e-safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications within our school and the community.

### **Use of the Internet**

Internet use is a part of everyday life for education, business and social interaction. In schools it is a statutory part of the National Curriculum in Wales and a necessary tool for learning. Therefore, our school has a responsibility to provide our pupils with Internet access as part of their learning experience. The purpose of Internet use at Llanbedr Church in Wales Primary School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions

Through internet use the school is able to access national and worldwide educational resource; access experts in many fields via email and online conferencing and communications; enhance learning and extend educational opportunities and experiences. Pupils will therefore be taught what internet use is acceptable and what is not and given clear objectives for internet use. Our school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law. Staff will evaluate web content used in lessons and activities for suitability before giving access to pupils. Pupils will be clear on the school procedures for reporting unsuitable content.

### **Information System Security and Filtering**

The school ICT systems, capacity, security and virus protection is the responsibility of the LA and in particular iteach. Llanbedr Church in Wales Primary School will work with Powys County Borough Council to ensure that systems to protect pupils are reviewed and improved.

"iteach" offer an award winning content filter which will ensure everyone is kept safe online - whilst allowing greater control over content.

This offers transparency of network traffic and access to archived reports, web based portal for easy access to settings, category based web filtering realtime monitoring & updates, BYOD Compatible.

Firewall and Security our internet connection includes a range of built in, always on security technologies, Network Intrusion Detection & Prevention Block Port Forwarding & Proxy Avoidance Attempts, Detect and block VPN connections.

If staff or pupils discover unsuitable sites, the URL must be reported to the e–safety co-ordinator. The school’s broadband access will include filtering appropriate to the age and maturity of pupils.

The school will take all reasonable precautions to ensure that users only access appropriate material on the internet. However, due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Any material that the school believes is inappropriate or illegal must be reported to the LA and if necessary to the appropriate agencies such as Internet Watch Foundation (IWF) or the Child Exploitation and Online Protection centre (CEOP).

## **Use of Email**

Members of Llanbedr Church in Wales Primary School may only use the approved ‘Outlook’ / Office 365 school email accounts provided by Powys County Borough Council / Crickcluster to communicate during school time for purposes related to education unless agreed by the head teacher. Pupils are not allowed to access their own personal email or communication accounts using the school network system. Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper.

The school website will only be used to communicate public information of which should be considered from a school security viewpoint. The contact details on the school website are the school address, email and telephone number. No other email addresses are to be published on the school website. Staff or pupils’ personal information must not be published.

In order to further secure pupil’s personal information, the publishing of pupils’ full names with their images is **not acceptable** on our website. Pupils must have parental permission before their work or photograph can be published on the school website. These permissions must be updated annually. Images that include pupils will be selected carefully and will not provide material that could be reused.

## **Recommendations and Policy**

At Llanbedr Church in Wales Primary School, we remind all staff about the lack of privacy and potential for unsavoury content with respect to social networking, Web 2.0 sites and blogs. As such, we actively remind all members of staff and the school community that they must be careful about the information they post due to potential security risks. Gwent Police have provided the following helpful advice concerning Social Networking sites:

- *Only use them if absolutely necessary*
- *At the very most use only your first name for the profile*
- *Do not put your date of birth on the profile*
- *Be wary about what pictures you put online of yourself, family and friends*
- *Make your profile “Invite only” so that you only allow people you trust with certainty*
- *to view your information*

- *Do not discuss political views*
- *Do not discuss work*
- *Do not post your occupation*
- *Be careful what viewpoint you express*

The internet offers a huge learning and teaching potential but at the same time, a breach of internet safety guidelines e.g. through the use of social networking, external webpages etc. can lead to a breach of trust and possibly bullying. Bullying of any kind is unacceptable at our school. If bullying does occur, all pupils and staff should feel comfortable to report it and know that incidents will be dealt with promptly and effectively.

### **What is Social Networking, Web 2.0 and Blogging?**

Social Networking has very much become a part of everyday life. Many individuals use it on a daily basis. In terms of communication via the internet, the use of social networking websites e.g. Facebook, Twitter, Instagram, Flickr will often surpass email use. Despite the popularity of social networking sites there are a number of potential risks about their use. It is also important to stress that once something is put onto the internet it can be very difficult to remove and there is a possibility that anyone can gain access to it.

Web 2.0 is the term given to the second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. The term 'Blog' is short for 'web log'. A blog is an online diary detailing personal insights and experiences, which is shared with an online audience.

All staff in school must think carefully about any information they post on a personal web space or blog, as this can be added to other peoples' pages and in turn passed on to others. The information posted will reflect the kind of person they are, which is why no information relating to staff, children or the wider school community should be shared or published by this means. Most social networking sites/ email accounts and the like, state that a person has to be aged 13 or over to have an account. Under no circumstances should teachers or staff authorise such an account for pupils and should endeavour to educate pupils in this area to raise awareness. Only social networking sites/ email accounts authorised by the Headteacher are to be used in school.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM (Instant Message) and email addresses, full names of friends/family, specific interests and clubs etc. Staff should also check the privacy settings on their profile and set them to private, checking the contact and friends list from time to time to make sure they still want them to know their personal details.

Staff should protect their password at all times. All staff working in schools should maintain an appropriate level of professional conduct in their own internet use, both within and outside school. Staff should note the recommendations of the e-safety

policy, guidance from the LA and ERW and also refer to the Code of Professional Conduct and Practice for Registered Teachers.

At Llanbedr Church in Wales Primary School all members of our school community are requested not to put any photographs of members of the school community onto an external website unless they have had prior permission. We also ask that in order to further protect the privacy, safety and well-being of our children, staff and community, that at no point should members of the school community engage in dialogue on such sites which relates to the school, children, staff or members of the extended school community. The school has a website, the FOS and school have Facebook pages, where matters relating to the school and it's wider community can be published.

## **Communication**

### **Pupils**

All users will be informed that the network and internet will be monitored. Staff will be trained to use the ThinkUknow resources online provided by CEOP (Child Exploitation and Online Protection).

Safe and responsible use of the internet and technology will be reinforced across the curriculum, including PSHE and citizenship covering both home and school access. Particular attention will be given where pupils are considered to be vulnerable. The school will organise e-safety weeks for pupils and e-safety workshops for parents.

### **Staff**

The E-Safety Policy will be formally introduced and discussed with staff and governors.

All staff are to be aware that internet traffic can be monitored and traced back to the individual user. Discretion and professional conduct is essential. A staff member will attend up to date training provided by SWGfL and Powys.

E-safety lessons can be accessed through the website for teachers to prepare for pupils ([swgfl.org.uk](http://swgfl.org.uk)).

### **Parents**

Parent and Carers attention will be brought to the e-safety policy in newsletters, the school Handbook and on the school website.

## **The Data Protection Act (1998)**

All members of the school community have a legal duty to protect the privacy of information relating to individuals. The Data Protection Act therefore applies to anyone who handles or has access to information concerning any individual. The

Act also allows individuals find out what information is held about them. The Act sets out eight principles that must be adhered to when handling personal data.

Personal Data must be:

- Kept secure;
- Processed in line with individual's rights;
- Processed fairly and lawfully;
- Processed for specific purposes;
- Accurate and up-to-date;
- Adequate, relevant and not excessive;
- Held no longer than necessary;
- Transferred only with security measures.

### **Prevention**

We will use a number of methods to help children and staff prevent a breach of these e-safety guidelines:

- Information sharing from the ERW (when available)
- Staff/Community training (supported by the ERW)
- Development of e-safety rules (relevant to our children)
- Regular e-safety lessons for our pupils ( delivered by teaching staff)

Although schools are not directly responsible for bullying off their premises we would encourage pupils, staff and members of the school community not to suffer in silence. We will always listen and take appropriate steps to address the issue.

The Headteacher, Mrs L.J.Green, is the child protection officer but all staff are responsible for implementing this policy. The policy will be shared with all staff and any new member of staff will receive a copy as part of their induction training. This policy will be reviewed annually.

### **New Technologies**

New devices and software will be evaluated for educational benefit and a risk assessment will be carried out before use in school. Devices already in the school such as iPads that connect to the internet will be used with clear guidelines and accessed through the school network only.

### **Procedures**

Our aim is to keep all pupils, members of staff and the wider school community safe and , if possible, change the behaviour of any person who may be using the internet inappropriately.

Procedures to be followed include:

- Report any suspect breach of internet e-safety guidelines to the Headteacher;
- All staff will be made aware of those pupils who cannot have their photographs shared on videos or social media. All staff should take this information into account when using the school website or Facebook;

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure;.
- Any complaint about staff misuse must be referred to the Head Teacher;
- All E–Safety complaints and incidents will be recorded by the school — including any actions taken;
- Discussions will be held with the local Police Community Support Officer to establish procedures for handling potentially illegal issues;
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

## **Authorising Access to the Internet.**

### **Staff**

All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

### **Foundation Phase**

Access to the Internet will be by adult demonstration and directly supervised access to specific, approved online materials.

### **Key Stage 2**

Pupils should be able to access the internet independently under supervision by a member of staff. Pupils and parents should discuss and agree and sign the Acceptable Use Policy and have a clear understanding of e-safety rules. Parents will be asked to sign and return a consent form for pupil access.

### **Writing and Reviewing**

The e-Safety Policy relates to other policies including those for ICT, bullying and for Child Protection.

The school's e-safety co-ordinator is Mr John.

The Policy will be reviewed annually by the e-safety coordinator and the Governing Body.

### **Equal Opportunities**

Llanbedr Church in Wales Primary School is committed to equality, including racial equality, for all members of the school community. The school promotes a positive and proactive approach to valuing and respecting diversity, and will not tolerate racial harassment of any kind.

## Acceptable Use Agreement: Staff (and also Governors, FOS and Visitors in respect of school duties).

### Staff, Governor, PFA and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body. This also includes any media form that contains the School Name and / or logo.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of CRICKCLUSTER /LEA/Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are areas to indicate this.
- I understand this forms part of the terms and conditions set out in my contract of employment.

#### User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

## Acceptable Use Agreement: Pupils - Primary

### Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes
- I will only use my class email 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 contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- I will not sign up to online services until I am old enough



Llanbedr Church in Wales School

*Ysgol Llanbedr*

Crickhowell, Powys, NP8 1SR      Crug Hywel, Powys, NP8 1SR

Tel: 01873 810619      Ffôn: 01873 810619

email: [office@llanbedr.powys.sch.uk](mailto:office@llanbedr.powys.sch.uk)

[www.llanbedrciw.org](http://www.llanbedrciw.org)

Headteacher: Mrs L.J.Green      Chair of Governors: Cllr E. Lusted

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Headteacher.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

.....✂.....

**Parent/ carer signature**

We have discussed this document with .....(child's name)  
and we agree to follow the e-Safety rules and to support the safe use of ICT at  
Llanbedr Church in Wales Primary School.

Parent/ Carer Signature .....

Class ..... Date .....