

CRYNALLT PRIMARY SCHOOL

E- SAFETY POLICY



Crynallt Primary School e Safety Policy is based on guidance given by the LEA. It provides details of how we as a school will implement and safeguard procedures relating to e safety. It is also based on material from BECTA and the Child Exploitation Online Protection (CEOP).

The school policy will cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. This policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school's e safety policy will operate in conjunction with others including policies for Pupil Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security plus any Home School Agreement.

Our e-safety highlights effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils.
- A comprehensive, agreed and implemented e- safety policy
- Secure, filtered broadband from the Neath Port Talbot Network
- A school network that complies with the Lifelong Learning Network Wales standards and specifications.
- The e safety policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and child protection.
- The schools e safety policy will be led by the head teacher who will work closely with the ICT coordinator.

Teaching and Learning

Why the internet and digital communications 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 a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will benefit education:

- The use of the internet benefits education. This is both through inclusion in the Lifelong Learning Network Wales which connects schools in NPT, and also through access to world-wide educational resources including museums and art galleries;

- It is also valuable for the exchange of curriculum and administration data (including SIMS) with the LEA and WAG.

Internet use will enhance learning

- School internet access will be designed expressly for pupil use and will include filtering, appropriate to the age of the 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;
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content:

- Crynallt Primary School will ensure that the use of the internet materials derived by staff and pupils complies with copyright law;
- Pupils will be taught the importance of cross-checking information before accepting its accuracy;
- Pupils will be taught how to report unpleasant internet content (e.g using the CEOP Report Abuse Icon).

Managing Information Systems

Information system security:

- The school ICT systems security will be reviewed regularly;
- Virus protection will be updated regularly;
- Security strategies will be discussed with the Local Authority.

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;
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission;
- The forwarding of chain letters is not permitted;
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known;
- The school should consider how e-mail from pupils to external bodies is monitored, presented and controlled.

Published content and the school web site:

Staff or pupil personal contact information will not be published. The contact details given online should always be the school office.

Publishing pupils images and work:

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. We will consider using group photographs rather than full face photos of individual children.

Ideally images should contain at least three faces with no name identification;

- The full names of pupils will not be used anywhere on a school website or other on-line space, particularly in association with photographs;
- Written permission from parents or carers will be obtained before photographs or any other details of pupils are published on the school web site;

- Work can only be published with the permission of the pupils and the parents/carers;
- Pupil image file names will not refer to the pupil by name;
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking and Personal Publishing.

- Social Network sites and newsgroups will be filtered/banned unless a specific use is approved;
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their 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.

Managing Filtering

- The school will work with the LLAN ICT sub group to ensure systems to protect pupils are reviewed and improved;
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator;
- Senior staff will ensure that regular checks are made to ensure that the filtering methods are appropriate, effective and reasonable.

Managing Video-conferencing and webcam use

- Video conferencing should use the education 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.

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;
- 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 material and communications;
- Mobile phones will not be used during lessons or formal school time. They can be kept for pupils by staff if needed at the end of the day. However, no responsibility for their safekeeping is held by staff.
- The sending of abusive or inappropriate text messages by files by Bluetooth or any other means is strictly forbidden;
- The use by pupils of cameras in mobile phones by pupils is strictly forbidden.

Protecting Personal Data

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

Policy Decisions

Authorising Internet Access

- 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;
- Parents will be asked to sign and return a consent form;
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 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 will 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;

Handling e-safety complaints;

- Complaints of internet misuse will be dealt with by a senior member of staff;
- Any complaints 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
- Pupils and parents will be informed of consequences for pupils misusing the internet;
- Discussions will be held with the Community Police Officer to establish procedures for handling potentially illegal issues.

How do we respond?

The Child Protection or e safety Coordinator can provide guidance should you be concerned about the internet use by a child, young person or member of staff.

The flow chart on the next page illustrates the approach to resolving an incident of concern. This diagram should not be used in isolation and the Education and Children's Services and the Local Safeguarding Children Board can provide supporting documents to assist schools when responding to incidents (Please see accompanying Incident of Concern Sheet)

Communications Policy

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 be informed that network and internet use will be monitored and appropriately followed up;
- A programme of training in e-safety will be developed;
- E-safety training will be embedded within the ICT scheme of work and the PSE curriculum.

Staff and the e-Safety policy

- All staff will be given the e-safety policy and its importance explained;
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user;
- Staff that manage filtering systems or monitor ICT use will be supervised senior management and work to clear procedures for reporting issues;
- Staff will always use a child-friendly and safe search engine when accessing the World Wide Web with pupils.

Enlisting parents' and carers support

- Parents' and carers attention will be drawn to the school e-safety policy in newsletters, and the school prospectus;
- The school will develop and 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.

This policy will be reviewed and amended in the Autumn Term 2020 or sooner if new technologies make it necessary

Signed: _____ (Chair of Govs)

Signed: _____ (Headteacher)