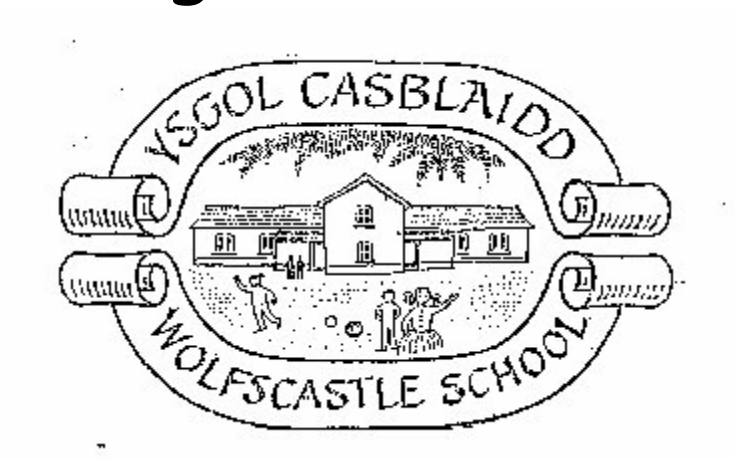
Ysgol Casblaidd



Wolfscastle C.P School

E-Safety Policy

"Dyro dy law i mi ac fe awn i ben y mynydd."

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement

• Illegal downloading of music or video files
• The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in our school. We recognize that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. The policy also explains how we attempt to inform those people who work with our children beyond the school environment (parents, friends, community) to be aware and to assist in this process.

Our school's e-safeguarding policy has been written from advice provided by Pembrokeshire County Council's Local Authority.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT

Responsibilities: the e-safety committee

Wolfscastle Primary School has an e-safety coordinator – Mrs Wendy Raymond however e safety at school is everyone's

responsibility. Teaching staff and the School Council meet on a termly basis to

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to Mrs Raymond other school staff as appropriate and when necessary to the ICT department of Pembrokeshire County Council.

Responsibilities: e-safety coordinator

Mrs Raymond our e-safety coordinator is the person responsible to the staff and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- leads the e-safety in the school community as well as discussions on e-safety with the School Council
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with Local Authority ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

 meets with e-safety governor to discuss current issues, review incident logs and filtering change control logs
 attends relevant meetings and committees of Governing Body
 reports regularly to staff
 receives appropriate training and support to fulfil their role effectively
 maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Responsibilities: governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

 regular meetings with the E-Safety Co-ordinator Mrs Raymond with an agenda based on:

- monitoring of e-safety incident logs
- monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices
- reporting to relevant Governors committee / meeting

Responsibilities: head teacher

 The head teacher is also the e safety co-ordinator and is responsible for ensuring the safety (including the day to day responsibility for e-safety) of members of the school community.

 The head teacher and assistant teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. see flow chart on dealing with e-safety incidents – below and relevant Local Authority HR /disciplinary procedures)

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

 they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

 they have read, understood and signed the school's Acceptable Use Policy for staff

 they report any suspected misuse or problem to the E-Safety Co-ordinator Mrs Raymond

 digital communications with students (email) should be on a professional level and only carried out using official school systems

 e-safety issues are embedded in the curriculum and other school activities.

Policy development, monitoring and review

This e-safety policy has been developed from advice provided by Pembrokeshire County Council

made up of:

 Head teacher /School E-Safety Coordinator

  Assistant Teacher

 Teachers

 Teaching Support Staff
 Governors (especially the e-safety governor)
 Pupils

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the:

e-safety coordinator together with the Assistant teacher, members of the School Council and the e safety governor.

Monitoring will take place at regular intervals: Annually

the governing body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:

Annually

The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:

November 2017

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

Pembrokeshire Safeguarding Children

Pembrokeshire Local Authority e-safety representative

Dyfed- Powys Police

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors,) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign as part of the Home School Agreement before being given access to school systems.

The Home School Agreement is revisited and resigned annually at the start of each school year and amended

accordingly in the light of new developments and discussions with the children which take place at the time.
Copies are sent home for further discussion with parents.
For children in EYFP & FP parents may sign on behalf of their children

Self Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school. The views and opinions of all stakeholders (pupils, parent, teachers) are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

ICT Policy How ICT is used, managed, resourced and supported in our school
E-Safety Policy How we strive to ensure that all individuals in school stay safe while using ICT. The e safety policy constitutes a part of the ICT policy.

Other policies relating to e-safety

Anti-bullying How our school strives to illuminate bullying – link to cyber bullying
PSHE E-Safety has links to this – staying safe

Safeguarding- Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy

Behaviour Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred

 threatening behaviour, including promotion of physical violence or mental harm
 any other information which may be offensive to colleagues or breaches the integrity of the ethos of the
school or brings the school into disrepute
Additionally the following activities are also considered unacceptable on ICT kit provided by the school:
 Using school systems to run a private business
 Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Pembrokeshire County Council and / or the school
 Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
 Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
 Creating or propagating computer viruses or other harmful files
 Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
 On-line gambling and non-educational gaming
 Use of personal social networking sites / profiles for non-educational purposes
If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that

correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Staff sanctions

Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Audit / Monitoring / Reporting / Review

The E-Safety coordinator will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the head teacher / and a governor on a termly basis.

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its

stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
  - Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
  - Members of staff are free to use these devices in school, outside teaching time.
- Pupils are not currently permitted to bring their personal hand held devices into school.

Email

Access to email is provided for all users in school via the intranet page accessible via the web browser (internet Explorer) from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school.

 A structured education programme is delivered to pupils which helps them to be aware of the dangers of
and good practices associated with the use of email.
 Staff may only access personal email accounts on school systems for emergency or extraordinary purposes
(these may be blocked by filtering).
 Users must immediately report, to their class teacher / e-safety coordinator – in accordance with the
school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
 Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.

 Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
 Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

Use of web-based publication tools

Our school uses HWB Cymru https://hwb.wales.gov.uk/ for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children.

All users are required to consider good practice when publishing content.

 Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
 Only pupil's first names are used on the website, and only then when necessary.
 Detailed calendars are not published on the school website.
 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:

- pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE

. Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Filtering

Introduction

Pembrokeshire County Council provides the filtering of internet content which is an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school community is aware of how to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the AUP (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through esafety awareness sessions / newsletter etc.

Monitoring

- No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- the e-safety governor
- Pembrokeshire County Council

E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's esafety provision. Children need the help and support of the school to recognise and avoid esafety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:
Using the 360 degree safe, Online Safety self-review tool for schools. This tool provides:

- Information that can influence the production or review of online safety policies and develop good practice.
- A process for identifying strengths and weaknesses.
- Opportunities for commitment and involvement from the whole school.
- A continuum for schools to discuss how they might move from a basic level provision for online safety to practice that is aspirational and innovative.

A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- We use the services of our Pembrokeshire School Community Police Officer P.C. Helen Llewellyn as a basis for our e-safety education
- Learning opportunities for e-safety are built into the Knowledge and Understanding sections of the FP curriculum
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
  - Checking the likely validity of the URL (web address)
  - Cross checking references (can they find the same information on other sites)
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy.

Governors should take part in e-safety training / awareness sessions, with particular importance for those who

Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, school handbook
- Parents evenings

Policy to be reviewed November 2017