PENYRHEOL COMPREHENSIVE SCHOOL

E-Safety Policy

UNCRC - Article 19

Young people have the right to be kept safe.

CONTENTS

RATIONALE

This School E-Safety Policy is intended to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies. This document outlines current agreed school procedures and duties already carried out by staff.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> "That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Penyrheol has made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, through our e-safety policy, we will try to ensure that we meet our statutory obligations to ensure that the children and young people in our school are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

SCOPE OF THE POLICY

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) 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 students / 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.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

The School Governors have been responsible for the approval of the E-Safety Policy and for reviewing the sanctions. Periodic reviews will be carried out during Curriculum or Personnel governor's meetings. During these meetings, information about e-safety incidents and monitoring reports will be given to those attending the meeting as and when required.

The current E-Safety Governor is – Mr Graham Ashman

The role of the E-Safety Governor may include:

- Meetings with the E-Safety Co-ordinator / Officer
- Monitoring of e-safety incident logs
- Monitoring of filtering / change control logs
- Reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the ICT Co-ordinator / Network Manager / Safeguarding & Child Protection Officer.
- The Headteacher / Senior Leaders are responsible for ensuring that the ICT Co-ordinator / Network Manager / Safeguarding & Child Protection Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team may receive regular monitoring reports from the ICT Co-ordinator / Network Manager / Safeguarding & Child Protection Officer.
- The Headteacher and another member of the Senior Leadership Team 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 (LEA guidelines for the City and County of Swansea will be followed in this case).

ICT Coordinator and Network Manager

The day to day responsibility for e-safety falls under the remit of the ICT Coordinator and Network Manager. However, ICT teachers and other teaching staff must also be continually vigilant and report issues immediately to the ICT Coordinator and Network Manager. Together these two staff will:

- take day to day responsibility for e-safety issues and have a role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- create a log of incidents to inform future e-safety developments
- meet regularly with the E-Safety Governor to discuss current issues
- reports regularly to Senior Leadership Team

The ICT Coordinator and Network Manager will ensure that any reported issues are brought to the attention of the relevant Head of Year and Senior Leadership Team members.

Network Manager / Technical staff:

In addition to liaising with the ICT Coordinator with regards to day-to-day e-safety issues, the Network Manager and ICT Technician will be responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined by LEA policies and the LEA Acceptable Usage Policy
- that users may only access the school's networks through a properly enforced password protection system, in which passwords can be regularly changed (pupils are prompted periodically).
- the LEA is informed of issues relating to Internet filtering concerns
- the school's filtering system is applied and updated on a regular basis
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the relevant HoY, classroom teacher, ICT Co-ordinator and members of the SLT.
- that monitoring software / systems are implemented and updated.

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 Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the ICT Coordinator and Network Manager/ICT Technician
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities (ICT lessons, DCF relevant cross curricular tasks, PSE sessions, assemblies delivered by SLT).
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (this is currently being strengthened via the development of the DCF across the school)
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use.

Safeguarding and Child Protection Officer

A Deputy Head is the current person allocated this role and should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign to allow them to have continued access to school systems.

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, family learning events, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy

Community Users and external education providers

Other users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems.

POLICY STATEMENTS

Education – students / pupils

E-Safety education at Penyrheol Comprehensive is provided in the following ways:

- A planned e-safety programme is part of ICT lessons and mainly covered in Years 7 – 8 ICT lessons. This follows aspects of the Digital Competence Framework. DCF sections covered are indicated on the DCF Mapping spreadsheet *(R:\DEPARTMENT AREAS\Digital Competence Framework\DCF Mapping Tool – Summary.xlsx)*
- PSE days have a rolling programme of E-Safety themes delivered by in-house staff and outside agencies.
- Pupils opting for GCSE ICT and Computer Science cover additional E-Safety topics to those covered in Year 7/8 ICT lessons and whole school PSE sessions.
- E-Safety themed assemblies are also delivered periodically to pupils by a member of the SLT
- Staff across all subject areas are currently developing DCF relevant resources. Some of which will cover E-Safety topics.
- AUPs in pupil planners are discussed with form tutors at the start of each academic year. Pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. Both they and their parents are then expected to sign the ICT AUP in their planners. Form tutors are expected to track this.
- Rules for ICT rooms are placed inside KS3 booklets and are recapped at the start of each academic year.
- ICT room displays are expected to feature rules for use of ICT rooms, the Internet and the school network
- Staff are expected to act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers (extended school)

The school has recently developed a yearly programme (2016 onwards) of Family Learning sessions. Within these sessions there is an E-Safety theme to assist parents with their own knowledge and reinforcement of E-Safety at home.

Additional information is also sent to parents via email, newsletters and via the school website. The school website has recently had a blog area added to it. Parents can subscribe to receive updates as and when the school adds relevant E-Safety information.

Education & Training – Staff

Staff will be given regular information and training on e-safety issues
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training may be given in the following ways:

- dissemination of e-safety updates through the weekly/daily school bulletin
- discussion of current e-safety issues through the DCF School Improvement Group. This group will then pass information to all other departments in the school.
- opportunities provided via inset training sessions
- Child Safeguarding training provided periodically by members of the LEA
- advice and training provided as required by individuals.

Training – Governors

Governors will be given regular information and training on e-safety issues
In the following ways

- opportunities arising at Governors meetings
- Child Safeguarding training provided by the LEA specifically for Governors.

A record of Governor training is kept up-to-date by the school

INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities. This will be achieved by ensuring:

- the School ICT systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in LEA policies and Acceptable Usage Policy and any relevant Local Authority e-safety policy and guidance
- there will be regular reviews of the safety and security of school ICT systems
- servers, wireless systems and cabling are securely located and physical access restricted
- all users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be regularly checked

- all users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be reminded to change their password periodically
- access to the Hwb Learning Platform will be monitored by the external providers of Hwb and the Network Manager. Pupils and staff will be given individual usernames and passwords along with restricted access levels suiting their usage requirements.
- users are responsible for the security of their own username and password, must not allow other users to access the systems using their log on details and are expected to immediately report any suspicion or evidence that there has been a breach of security.
- the school monitors and supports the externally managed Internet filtering service provided by the LEA.
- any filtering issues will be reported immediately to the LEA ICT support service
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (please see GDPR regulations and CCOS Data Protection policies for further detail).

Use of digital and video images - Photographic, Video

Please refer to the CCOS policy on the use of images.

Data Protection

Please refer to the CCOS policy on GDPR.

Communications

The school currently has separate Mobile Phone Usage and Twitter usage policies available upon request.

LEGISLATION

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:
• Erase or amend data or programs without authority;
• Obtain unauthorised access to a computer;
• "Eavesdrop" on a computer;
• Make unauthorised use of computer time or facilities;
• Maliciously corrupt or erase data or programs;
• Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
• Fairly and lawfully processed.
• Processed for limited purposes.
• Adequate, relevant and not excessive.
• Accurate.
• Not kept longer than necessary.
• Processed in accordance with the data subject's rights.
• Secure.
• Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is

complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.