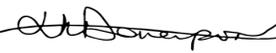




Ysgol Uwchradd
PRESTATYN
High School



E-Safety Policy

Author	Date Adopted by Gov Body	Signed by Chair of Gov	Review Date
DCC/PHS	15/7/15		July 2016
DCC/PHS	13/7/16		July 2017
DCC/PHS	12/7/17		July 2018
DC/PHS	12/7/18		July 2019

RATIONALE

This policy should be read in conjunction with the DDC Policies on E-safety for Schools, Use and Monitoring of the Internet. E-mail and Telephones for Schools, Safe Use of IT – A Guide for Teachers and Adults Working with Children, and Information Security Policy & Guidelines. As well as this policy, there are various laws that determine how computers should be used; The Computer Misuse Act 1990 and the Data Protection Act 1998

PURPOSE/PRINCIPLES

- To provide general and specific policies and protocols for the effective and legal use of all information and communications technology (ICT) equipment provided by Prestatyn High School.
- To support Headteachers, Managers and Leaders in establishing a culture which safeguards staff and students in Prestatyn High School.

BROAD GUIDELINES

- The policy covers the use of all computer equipment and applies to all employees of PHS including temporary staff, contractors, and consultants.
- All ICT facilities must be used in a professional manner, eg. emails to be drafted in a clear and unambiguous way so as not to cause offence to the recipient; and confidentiality of information held on computer databases be respected.
- All students must be equipped with the skills and knowledge they need to use technology safely and responsibly and be able to manage the risks, wherever and whenever they go on line.
- The policy applies to emails to both internal and external use of the medium and all intranet and similar electronic information exchanges.

MONITORING & EVALUATING

This policy will be subject to amendments in response to changing circumstances.

DEFINITIONS

IT equipment is defined as being:

'Any electronic equipment that is capable of storing or transmitting information.' This includes a range of digital technologies such as blackberries, webcams, e-mails etc.

LINKS TO OTHER POLICIES

Child Protection Policy
Equal Opportunities Policy
Anti-bullying Policy
Healthy Schools Policy

Ready to Learn Policy
Race Equality and Harassment Policy
Code of Safe Practice
PSHE Policy

Why is having Acceptable Use and E-safety Policies essential?

The use of Technology in schools bring great opportunity and the benefits of technology are an essential aspect of learning. Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high, their understanding of the risks may be low, alongside their ability to respond to any of the risks they encounter.

Schools now need to focus on equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online. Effective Acceptable Use and E-safety Policies can help to establish, and reinforce, safe and responsible online behaviours.

Classifying the risks

The Byron Review classifies e-safety risks as involving **content**, **contact** and **conduct**, illustrating that the risk element involved in using new technologies is often determined by **behaviours** rather than the technologies themselves. A child may be a recipient, participant or actor in online activities posing risk, as illustrated below:

	Commercial	Aggressive	Sexual	Values
Content Child as recipient	Adverts Spam Sponsorship Personal Info	Violent/Hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact Child as participant	Tracking Harvesting Personal Info	Being bullied, harassed or stalked	Meeting strangers or being groomed	Self harm Unwelcome persuasions
Conduct Child as actor	Illegal downloading Hacking Gambling Financial Scams Terrorism	Bullying or harassing another	Creating or uploading inappropriate material	Providing misleading info/advice

Schools must decide on the right balance between controlling access, setting rules and educating students for responsible use. Schools, libraries and youth services must develop complementary strategies to ensure safe, critical and responsible ICT use wherever the young people may be using IT.

E-safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education on risks and responsibilities and is part of the duty of care which applies to everyone working with children. A new national e-safety drive is

being led by the Child Exploitation and Online Protection Centre (CEOP) and detailed materials for schools are available from Becta. Unfortunately, at present there is little guidance available for Wales, but the following link will shortly contain information for practitioners in Wales.

What is e-safety?

The Schools e-Safety strategy should reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day. Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people.

In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others. Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to groom children.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is unauthorised. However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

Statement of authority

Through this guidance, Denbighshire County Council is making a strong statement as to the precautions that it expects schools to take with regards to e-safety.

Responsibilities of school staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-safety issues with pupils. Advice and training may be obtained from the Denbighshire ICT Adviser. Ask advisers or child protection coordinators if in doubt.

Nationally, CEOP has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders".

In the School a member of staff who flouts security advice, or uses e-mail or the Internet for inappropriate reasons risks dismissal. All staff should therefore sign the Acceptable Use Policy.

Staff thereby accept that the school can monitor network and Internet use to help ensure staff and pupil safety. Staff that monitor ICT use have great responsibility. Procedures must define how inappropriate or illegal ICT use is reported to senior management.

Staff must also be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source. Any allegation of inappropriate behaviour must be reported to senior management and investigated with great care. An innocent explanation may well exist. E-mail and text messaging all provide additional channels of communication between staff and pupils and inappropriate behaviour can occur, or communications can be misinterpreted.

All staff should ensure that they read the Internet, E-mail and Telephone usage policy for Schools and the DCC Safe Internet guide for Adults working with Children.

Identifying vulnerable groups

Many pupils have access to mobile devices. The use of handhelds and internet-enabled mobile phones both inside and outside school is increasing rapidly. The most ICT capable may be the most vulnerable. Children who have poor social skills may be more at risk from inappropriate online contact.

Principles behind Internet use

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the schools management information and business administration systems.

Internet access is an entitlement for students who show a responsible and mature approach to its use. The school has a duty to provide students with safe and secure Internet access as part of their learning experience. Students need to be taught what is acceptable and what is not and given clear objectives for Internet use.

Using the Internet to support learning

Most Internet use in schools is safe, purposeful and beneficial to learners. There is always an element of risk. Even a seemingly innocent search can occasionally turn up links to adult content or violent imagery.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils.

For example:

Close or minimise the image or window immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Report the matter to the e-safety co-ordinator and/or senior management.

In view of the risks, we advise that primary pupils are supervised at all times when using the Internet. All staff should be aware that networked computers are generally online at all times when a user is logged on.

Search engines

The BBC search engine is a safer approach for young children: <http://search.bbc.co.uk/>

Image searches are especially risky. There may be no need for pupils to download them, as long as an adult downloads the images before the lessons and stores them in a shared folder.

Alternatively, teachers may use Microsoft's clipart library, which automatically adds downloaded images to Clipart: <http://office.microsoft.com/clipart/>

Tagged image browsers are fun to explore. A good example is www.airtightinteractive.com/projects/related_tag_browser/. The danger is however that this will accept inappropriate keywords. While useful to teachers, we do not recommend it for use by pupils.

For most curriculum-related research, there is no need to use an unfenced search engine. Yahoo!igans, although US based, does offer a range of selected sites which are relevant to the UK curriculum. For details, see Yahoo!igans UK: <http://uk.docs.yahoo.com/yahooligans/parents.html>

Please note that NO filter-based search engine is completely safe.

Curriculum planning

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

If the aim is to teach search skills, BBC Schools offers a safe environment. The search box automatically restricts the search to the BBC Schools site. There is no indication of age range, but pupils can judge readability from the example retrieved by the search www.bbc.co.uk/schools. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Teaching e-Safety

The BBC Chat Guide site <http://www.bbc.co.uk/chatguide> contains a range of carefully designed teaching packs for KS2 and KS3. There are games and advice for children and young people and a downloadable ChatGuide booklet for parents.

CEOP's 'think you know' programme is an excellent resource and contains age related e-safety advice with interactive games and activities for all children and young people from the age of 5 upwards.

Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law, students should be made aware of plagiarism and issues relating to work research being undertaken for coursework.

E-safety for pupils with additional needs

There are certain aspects of teaching e-safety that are particularly challenging for pupils with additional needs and children who we may consider to be vulnerable in this learning context. Pupils will clearly have individual needs that will present a range of issues when teaching e-safety but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children
- They are likely to find it hard to apply the same rules in different situations
- Most safety principles rely on children being able to explain what happened or to ask for help
- Some children may have poor recall and difficulties with learning through experience

It would seem to be relevant for all schools to consider their e-safety policy in relation to pupils with additional needs. This may take the form of child-focused strategies that would apply to a pupil with specific needs and would be made available to all staff involved in Internet use with that child. Alternatively, whole school approaches could take into consideration strategies that would support the needs i.e. specific choices of visual support to remind pupils of the rules.

Response to an incident of concern

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school.

However, it is also important to consider the risks associated with the way these technologies can be used. An e-Safety strategy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from curiosity, prank or unconsidered action to illegal activity.

This section will help staff determine what action they can take and when to report an incident of concern. Matters can then be handed over to the appropriate service or the Police if that becomes necessary.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs)
- Internet research: websites, search engines and web browsers
- Mobile phones and personal digital assistants (PDAs)
- Internet communications: e-mail and IM
- Webcams and videoconferencing
- Wireless games consoles

What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing incitement sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information
- Hacking and security breaches
- Corruption or misuse of data

School responsibilities

As e-Safety is a relatively new concept and covers a wider scope than Internet use, a summary of a school's e-safety responsibilities might be useful. This list should assist in developing a co-ordinated and effective approach to managing e-Safety issues. The following should be considered:

- Encourage schools to appoint a person with e-Safety responsibilities. This may be the same role as the designated Child Protection Coordinator, but could also be a member of SMT, the ICT Coordinator or a subject teacher.
- The e-Safety co-ordinator should maintain the e-Safety strategy, manage e-Safety training and keep abreast of local and national e-safety awareness campaigns.
- Schools should review their strategy regularly and revise it annually to ensure that it is current and considers any emerging technologies.
- To ensure that pupils and staff are adhering to the strategy and related policies, any incidents of possible misuse will need to be investigated. Reports are available to assist in the routine monitoring of internet use at each School.
- Schools should include e-Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupil need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable Use Policy.
- Pupils and Parents should be asked to sign and return the Acceptable Use Policies. Suggested Acceptable Use policies for schools to adopt are included at appendix A. These can be tailored to your specific needs.

- The e-Safety strategy should be communicated and made available to all staff, governors, parents and visitors in line with normal school procedures.

Implementation and Compliance

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate educational ICT experiences.

The following ideas and checks may be useful:

- How are pupils reminded of their responsibilities? Displaying posters in rooms with computers is one useful approach.
- Do staff, pupils and parents know how to report an incident of concern regarding inappropriate use?

Prestatyn High School

E-safety Rules – Secondary School Pupils

These e-Safety Rules help to protect students by describing what is acceptable and unacceptable computer use.

- 🔒 The school owns the computer network and sets the rules for its use.
- 🔒 Irresponsible use by any pupil may result in the loss of network or Internet access.
- 🔒 Your user ID and Password must not be given to any other person, nor should you use anybody else's user ID and Password.
- 🔒 Copyright must be respected. You must not download any file, picture, game or programme that you know is copyright protected. If in doubt, ask a teacher.
- 🔒 Messages and e-mails must be written politely and you must not use words that could be abusive or offensive to other people.
- 🔒 Do not open e-mails or attachments that you suspect may contain a virus or malware.
- 🔒 Anonymous messages and chain letters are not permitted. Forwarding these to your friends may upset them.
- 🔒 You must take care not to reveal your personal information (your name, address or the school you attend) in an email, on a social networking site, by personal publishing, blogs or messaging.
- 🔒 Do not make arrangements to meet people you have met online without first checking with a parent or guardian.
- 🔒 The school ICT systems are to be used for educational purposes only, unless the head teacher has given specific permission to use them for recreational purposes i.e. at break times.
- 🔒 Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- 🔒 If you accidentally access any site you think is not suitable, report it to a teacher or member of School staff. Using proxy avoidance sites to intentionally access this material is not permitted.

The school may monitor the use of the school's computer systems, including access to the internet, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Pupil Agreement:

- I have read the e-safety rules and agree to abide by them.
- I will make sure that I use the school computers in a responsible way and understand that any misuse may result in the withdrawal of my IT use.
- I know that internet and network use may be monitored by my school who may report concerns about my use to my parents or guardians.

Name: Class:

Signed: Date:.....

To be completed by a Parent or Legal Guardian:-

Consent for Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published on the internet, for example the schools website.

I also agree that appropriate images and video that include my son/daughter may be published, but for safety reasons any photographs will not be accompanied by pupil names.

Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.

I understand that the school cannot be held wholly responsible for the content of external websites accessed and I will ensure my son/daughter is fully aware of the e-safety rules and that any misuse may result in withdrawal of network or internet access.

Signed: Date:.....