



Pontypridd High School

**e-safety and ICT Acceptable Use
Policy**

February 2018

Policy

Date of policy:	February 2017
Adopted:	Wellbeing Committee Meeting, Spring 2017 Reviewed 8 th March 2018, Learning and Teaching Committee Meeting
To be reviewed:	Spring 2020
Member of staff responsible:	Deputy Headteacher
Committee Responsible:	Teaching and Learning

Rationale

The very nature of this subject means that this policy must be as dynamic as possible and in constant review. Devices, new networks and the terminology associated with technology are developing all the time.

Our policy aims to balance the desirability of fully exploiting the vast educational potential of new technologies with providing safeguards against risks and unacceptable material and activities.

This policy considers all technological appliances used by pupils and includes;

- both fixed and mobile internet
- technologies that may have been provided by the School (such as PCs, laptops, tablets, webcams and digital video equipment);
- technologies owned by students, but brought onto school premises (such as laptops, mobile phones, iPads/android devices, camera phones).

Although a student may be trusted by his / her parents / carers with regard to private internet use, the School has a duty to safeguard them and other students.

The School believes in being proactive rather than reactive. Therefore supervision of technologies and educating pupils are key to enabling them to value the benefits of communication and exploration, whilst ensuring they understand the potential dangers associated and as such, are protected from them.

Aims

Students are keen to grasp the opportunities offered by new technology and their availability, portability, miniaturisation and use of sophisticated electronic devices. However, as with any new technology, there are associated risks which include the following:

- exposure to inappropriate material (e.g. pornography, violence, hate sites, self-harm sites)
- grooming
- identity theft (including 'fraud' - hacking Facebook profiles) and sharing passwords
- online cyber bullying
- digital footprint and online reputation
- health and well-being - amount of time spent online (internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGI (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership)

The School does not accept responsibility for, nor is insured against theft, loss or damage to any students' personal property, including electronic devices.

Procedures and Practices

The School provides students with Internet access and access to the School's own network through connections in classrooms. Every student has an individual username and password with the means to create and save files. We are mindful of the popularity of e-readers and devices such as iPads, some of which are perfectly suitable for education.

Rules and Regulations

The rules and regulations below offer a level of consistency and guidance across each area of the school.

- Students may only use the account assigned to them
- No student is allowed to email another student or member of staff unless it is school related
- No students may use ICT resources unless supervised appropriately
- The use of games is banned unless they have an educational purpose as deemed by the School
- Chat Rooms and social networking sites are not permitted
- Gambling and e-Commerce are not permitted
- Downloading or sharing of files such as music files is not permitted
- The use of inappropriate images / websites / video clips is not permitted
- The use of mobile phones, camcorders, digital cameras, e-readers, iPads/Tablets, MP3 Players and games consoles are not permitted unless students have permission
- Sending or taking data out of School is not permitted without explicit permission

Measures in place to support the policy

Induction

All students are inducted in appropriate use of the school's ICT facilities and other aspects of this policy by teachers of ICT.

Paperwork

This policy protects all parties by clearly stating what is acceptable and what is not. This is discussed and explained with all students. An agreement is signed and then kept in a file within the ICT department.

Education

All students undertake ICT lessons. A key component of these lessons is to achieve a greater understanding of the important issues of e-safety. We not only look at what is acceptable / unacceptable behaviour, but we also discuss the consequences of these actions. Material is age-appropriate and content is based on the CEOP recommendations.

Staff

Appropriate and relevant staff training takes place every year. It is not the responsibility of specific members of staff to be vigilant for any instances of concern. It is the responsibility of the all staff, whether that be on a school trips, at break times, in lessons or after school.

Parents

E-safety education / information is made available in parents / carers meetings each term. This is a crucial link to helping keeping children safe since many issues that are highlighted have occurred outside of school lesson time.

Other

Assemblies, PSE lessons and form groups all address cyber-bullying, safe use of the internet and appropriate use of technologies.

Monitoring and Sanctions

The school will exercise its right to monitor the use of computer systems, including the monitoring of internet use, interception of e-mails and the deletion of inappropriate materials at all times. In circumstances where the school believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the school reserves the right to inform appropriate authorities and provide documentary evidence.

Students should be aware that computer / mobile phone memory, e-mails and other forms of electronic information storage and communication (including any external storage media which pupils bring into the School) may be scrutinised for the purposes of safeguarding or promoting a child's welfare. This will be authorised by a senior member of staff.

Although all staff and students at Pontypridd High School are expected to use ICT responsibly and receive specific education to define and encourage responsible use, the school recognises that it has a responsibility to counter any attempts at irresponsible behaviour which may still arise. Thus, the school's ICT system is monitored and managed in a number of ways designed to inhibit abuses, specifically:

- Code of Conduct: All users agree to abide by the code of conduct (Appendix A)
- User Logons and Passwords – all users have their own private logons and password. These should not be shared with anyone else.
- Access rights to confidential data – Staff make every effort to ensure that all users understand that confidential data must be stored in folders controlled by appropriate access rights.
- Mail Filtering – keyword filtering prevents some inappropriate emails leaving the school or arriving into user mailboxes.
- Computer Logs – all user logon and logoff activity is logged. All website requests are logged and users are taught this.
- Social Networking sites – access to these is blocked.

Expectations of Students and Parents / Carers beyond the School

When a student is at home, families bear responsibility for the guidance of their children. The school expects the use of ICT by its students, even when at home, to comply with the school's stated ethos, and honour the agreement they sign permitting their use of ICT at the School. Material downloaded in the home, posted in cyber-space from a home computer, or transmitted to a mobile phone when a student is at home can impact significantly upon the life of students at School. Thus the school requires the parents / carers of students enrolled at Pontypridd High to co-operate with the school in the education of their children in the use of ICT.

- Most initial offences will be dealt with by Head of Faculty and the removal of computer or internet usage may be a first punishment. In such circumstances parents / carers may be notified.
- More serious offences or repeated abuse of ICT by a student will be dealt with by the Deputy Headteacher or Headteacher. In such circumstances parents / carers will be informed.
- When abuses of ICT constitute illegal activity, staff will interview the student with his parents / carers. Sanctions applied will be proportionate to the offence committed. This may also involve informing the police.

Responsibility

If a student comes across inappropriate or illegal material they must inform a member of staff immediately.. Reports about suspicious behaviour towards children and young people in an online environment will be made to the Child Exploitation and Online Protection Centre (CEOP). Law enforcement agencies and the service providers may need to take urgent steps to locate the child and / or remove the content.

NEVER forward content (email, photo, website address etc.) to someone else containing inappropriate content. This is an offence.

NEVER forward content (email, photo, website address etc.) to someone else containing illegal content. This is an offence.

Pontypridd High School – ICT Acceptable Use Agreement

All students, parents / carers must abide by the expectations set out in this policy. It details the ways in which the computer systems (including Internet and email) can and cannot be used. The school reserves the right to change this policy.

Computer Rooms

- No food or drink is to be taken into or consumed in these rooms
- Hands must be clean.
- Keyboards, mice, mouse mats, monitors, cables and chairs must be left in a good condition, ready for use by the next person.
- Noise levels must be kept to a minimum.
- Students are not to move keyboards or mice without permission

Printers

- Only print schoolwork.
- Only print when absolutely necessary.
- Make sure your name is on the work you are printing out.
- Always check that your work is finished (including spelling).
- Avoid wasting paper.
- Remember to collect your printouts from the printer.

Logging on

- You are only allowed to use your **own** "Username"
- You must use a password, which remains secret. Ask for help if you do not know how to change it.
- You must never borrow anyone else's Username or let someone else use yours.
- You must never attempt to alter system settings and software.
- You must not attempt to install software on the system.
- You must log off when leaving a computer to prevent others using your login.

Internet and E-mail

You must always behave in a responsible way, paying particular attention to the following:

- Never attempt to look for unsuitable / illegal pictures or information. If you find anything like this by accident, close down those pages **immediately**. Remember that the pages you visit, and for how long, are logged. **Tell a teacher what you have found.**
- Do not download unnecessary material. It can contain viruses and pictures which can take up a lot of disk space on the server.
- 'Chat rooms' and social networking sites, such as Instagram and Facebook are **not** to be used.
- The playing of games is **not** permitted unless of an educational nature and with staff permission.

- When using e-mail do not use bad language, unpleasant pictures or cartoons. Never send an e-mail that anyone else might consider offensive or inappropriate.
- Do not reveal personal details such as your name, age, address and telephone number to anyone online.

C-Touch / Interactive Whiteboards

- You must only touch or use them with staff permission.
- You must not use any type of ink pens on an Interactive Whiteboard.
- You must not stick anything to, poke or scratch a C-Touch / Interactive screen

Mobile Devices

This includes mobile phones, iPods, iPads, voice recorders and other devices that have the ability to record or show images, sounds or video. Students are allowed to bring mobile phones into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use;

- Mobile phones must be switched off in all classes, corridors and other areas during teaching time. It is not acceptable for phones merely to be put on silent or vibrate.
- The phone must be kept out of sight during lessons.
- No pupil may take a mobile phone into a room or other area where examinations are being held.
- The security of phone will remain the pupil's responsibility in all lessons
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.
- Mobile phones should not be used in any manner or place that is disruptive to the normal routine of the school.
- Students should only use their mobile phones before or after school or during break time and lunch breaks and only with permission of staff, so usage can be monitored at all times. This is to ensure safety for all.
- Students should protect their phone numbers by only giving them to friends and keeping a note of who they have given them to.

When in possession of a school mobile device then the following must be adhered to;

- No photographing or filming staff or other students without their knowledge or permission.
- No photographing or filming in toilets, changing rooms and similar areas.
- No bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging (including airdrop), sending inappropriate messages or posts to social networking or blogging sites.
- Do not use an iPad / laptop when the teacher has not given permission to do so in their lesson, or when you have been asked to stop using one.
- Do not borrowing a school iPad / laptop without permission from a member of staff
- Do not fail to return a school iPad / laptop that you have borrowed to the correct place
- Do not installing / removing an app or program on an iPad or laptop or altering/trying to circumvent the system settings.
- Do not use or carry an iPad or laptop in a careless manner that may result in damage being caused to it.

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile phone and a serious breach of the positive relationships policy resulting in sanctions being taken;

- Photographing or filming staff or other students without their knowledge or permission.
- Photographing or filming in toilets, changing rooms and similar areas.
- Bullying, harassing or intimidating staff or students by the use of text, email or multimedia messaging, sending inappropriate messages or posts to social networking or blogging sites.
- Using the mobile phone when the teacher has not given permission to do so in their lesson or when the classroom mobile phone sign is red.
- Refusing to switch a phone off or handing over the phone at the request of a member of staff.
- Using the mobile phone inside or outside school hours to intimidate or upset staff and students will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

Sanctions

Students and parents / carers are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines. In addition, the school is within its rights to confiscate the phone where the guidelines have been breached.

Using the mobile phone outside school hours to intimidate or upset staff and students or undermine the stability of the school in any way will be considered a breach of these guidelines in the same way as unacceptable use, which takes place in school time.

- If a phone is confiscated, school will make it clear for how long this will be and the procedure to be followed for its return.
- Students should be aware that the police will be informed if there is a serious misuse of the mobile phone where criminal activity is suspected
- If a student commits an act which causes serious harassment, alarm or distress to another student or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

Confiscation procedure

If a mobile phone is confiscated then :

- At the discretion of the teacher the mobile phone will be returned at the end of the lesson.
- The pupil will be informed that the phone can be collected at the end of school day from Pupil Services or nominated senior member of staff.
- The confiscation will be recorded in the school behaviour log for monitoring purposes.
- The School will ensure that confiscated equipment is stored in such a way that it is returned to the correct person.
- In the case of repeated or serious misuse the phone will only be returned to a parent / carer who will be required to visit the school by appointment to collect the phone. This may be at the end of a week, a half term or longer. At the discretion of the Headteacher the phone may be returned to the student at the end of the confiscation period.
- Where a student persistently breaches the expectations, following a clear warning, the Headteacher may impose an outright ban from bringing a mobile phone to school. This may be a fixed period or permanent ban.

Where the mobile device has been used for an unacceptable purpose

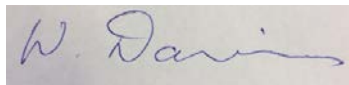
- The Headteacher or a designated staff member will have the right to view files stored in confiscated equipment and if necessary seek the cooperation of parents / carers in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.
- If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen
- The School will consider whether an incident should be reported to the safeguarding board.

- The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim, which needs further investigation.

Approved by:



Mr H Cripps, Headteacher



Mr W Davies, Chair of Governors

Pontypridd High School

Use of ICT Facilities – Acceptable Use Declaration

No pupil will be allowed use of the School Internet and E-mail facilities unless both they and their parent/carer have completed this form. In addition, they will not be allowed to use the Computer Room in 'free time' unless this form has been completed.

STUDENT

I have read and accept the Acceptable Use Policy.

I agree to comply with the school rules on the use of all ICT facilities. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Student Signature :Date :

PARENT / CARER

I have read and accept the Acceptable Use Policy.

As the parent or legal carer of the student signing above, I grant permission for him / her to use all ICT facilities including electronic mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for him/her to follow when selecting, sharing and exploring information and media.

Parent / Carer Signature :Date :

Name of Student :