Ponteland High School

ICT Acceptable Use and E-Safety Policies

2023-24

Last updated September 2023

Secondary School Core Policy

The senior leadership team has approved this e-Safety Policy to be used by the school.

Contents Page

ICT Acceptable Use Policy

E-safety policy

ICT Acceptable Use Policy for Ponteland Community High School

Student User Agreement

The school's computer system is provided in order to support the work of students and teachers. Our intention is that the system will be used creatively and to the benefit of all. To enable this, it is important that all people who use the school's computers and computer network accept certain responsibilities and adhere to certain requirements. These responsibilities and requirements are stated in this policy. **When using the school's computer resources and network all users must abide by the acceptable use rules.**

Use of the school's computer systems is always conditional on observing and adhering to the Acceptable Use Policy. Students will be reminded of this in class and the details will be reviewed in lessons and assemblies. However, we request that all students read the Acceptable Use Policy with a parent and that the child ticks the box and inserts their name at the bottom of the Google Form. This is to acknowledge that they have been given the opportunity to read the policy and understand its implications and requirements.

Thank you

Mr M Warland

Deputy Headteacher

ICT Acceptable use policy for Ponteland Community High School 2023-24

1.1 Computer and Audio Visual equipment

- You must use the equipment provided with care to ensure the risk of damaged is minimised.
- Report any damage to equipment immediately to a class teacher of the ICT team (it-support@ponthigh.org.uk).
- Make sure you sign for the receipt of equipment when asked.
- Any equipment assigned to you is your responsibility; you are responsible for any misuse or damage.
- Students must not install software on any school computer system.
- Students may bring their own equipment into school to use at the discretion of the class teacher on the understanding they are responsible for its security and safety. The school does not provide any insurance for loss or damage of personal equipment. However, any loss or damage in school should be reported to a teacher as soon as possible.
- The mobile devices and phones of students in Years 7,8, 9, 10 and 11 must be switched off and kept out of sight throughout the school day. The exception to this is where a teacher gives permission for a device to be used as part of a supervised activity during a lesson.
- Do not take pictures, videos or audio of other students or adults without getting their permission beforehand.
- Never use mobile phones or cameras in the school toilet areas.
- As a matter of courtesy, Post 16 students must not use their phones when walking in the corridors or in lessons without the explicit permission of their teacher.

1.2 ICT network

- Make sure you know your computer logon details, including your password.
- Change the password you are provided with when you first logon to one that only you know.
- Never tell other people your computer password or let anyone else logon to your user accounts. You will be responsible for any abuse or misuse that results.
- Always check that you have logged off properly when you have finished using the computer.
- The computer network must not be used for computer gaming, unless authorised by the supervising member of staff.

- Any attempt to access an unauthorised ICT system (hacking) will be deemed a breach of this policy.

1.3 Communications

- Various communication systems are provided by the school, including email, messaging and access to internet based email.
- We expect everybody to use the communication systems with care and consideration of others.
- School email accounts should be used for school related business only.
- Avoid causing offence, do not send offensive material to others.
- Report any unsuitable material that is sent to you to the class teacher, form tutor or ICT technician.
- Report any incidents involving cyber-bullying to the class teacher, form tutor, pastoral manager or ICT technician/Manager.
- The school reserves the right to filter all email for inappropriate material and Spam.

1.4 Internet

- Access to the internet is provided so that students and staff can use it as a source of information and resources. We take steps to protect students and staff from accessing inappropriate information and images through filtering and monitoring systems.
- All school computers (staff and students) have safeguarding software installed which monitors the text displayed on the screen including personal email accounts. If the software identifies text related to a range of sensitive topics then a screenshot is taken as evidence and the Headteacher is informed.
- Take care when searching for information that is appropriate for use in school.
- Do not abuse the internet facility by deliberately searching for and/ or downloading offensive materials or materials inappropriate for use in schools
- You must not attempt to bypass school and NCC internet filters by using proxy sites to access internet sites.
- Remember that it is a criminal offence to deliberately gain access to secure sites on the internet or to try to cause damage to systems (hacking).

1.5 Monitoring use

- As a public organisation with responsibility for the care of young people we will exercise our right to monitor the use of our computer systems for inappropriate use.
- In order to protect our students and staff from inappropriate material we use a number of methods of monitoring use. These include remote monitoring of screen displays and recording of the internet sites accessed by users.
- We will only check user records when we believe that somebody has failed to fulfil their responsibilities.

1.6 Sanctions

- Inappropriate use of computers and the internet will result in one or more of a number of possible sanctions, including limitation or loss of internet access and loss of network access for a period of time deemed appropriate by the school.
- Individuals who carry out criminal actions will be reported to the appropriate authorities and the School will assist fully with any subsequent investigation.

(Additional points only relevant to members of staff)

In addition to the contents of the main ICT Acceptable use policy the following points also apply to all members of staff

(1.2) ICT network

- Do not install computer software onto the computer network unless you have been authorised to do so by the ICT technicians/Manager.
- Staff should not allow students unsupervised access to their account or computer.
- Students should not log onto staff computers / laptops.

- No personal or sensitive school data should be stored on unsecure local drives (C: , D:) ,or removable storage (memory sticks, DVD/CD's etc). All data should be stored on network drives where it is secure and can be backed up.

(1.3) Communications

- Report any offensive or inappropriate material that is sent to you or any student to a member of the Senior Leadership team as a matter of urgency. It constitutes a potential safeguarding issue.

E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Safeguarding, Student Behaviour, Bullying, Curriculum, Data Protection and Security.

2.0 School e-safety policy

2.1 Writing and reviewing the e-safety policy

- The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- The school will appoint an e-Safety coordinator. In many cases this will be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on the Becta eSafety and government guidance. It has been agreed by senior leadership and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually (or before if significant amendments are required).
- The record of review, updating and governor approval is recorded in the Revision matrix at the end of this document.

2.2 Teaching and learning

2.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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 students.

2.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.2.4 Students will be taught how to evaluate Internet content

- The school will endeavour to ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

2.3.1 Information system security

- The School's ICT system capacity and security will be reviewed regularly by the ICT co-ordinator and network manager.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority to ensure best practice is maintained.
- Unapproved system programmes, utilities and executable files will not be allowed in students' work areas or attached to e-mail.

2.3.2 E-mail

- Students will be encouraged to use approved e-mail accounts on the school system, the use of personal web mail accounts such as Hotmail may be blocked as appropriate.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be in a professional manner.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school website

- The contact details on the website will be the school address, e-mail and telephone number. Staff or students personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing students' images and work

- Photographs that include students will be selected with children's safety in mind.
- Students' full names will not be used anywhere on the Web site without express permission.
- Written permission from parents will be obtained before photographs of students and / or full names are published on the school Web site or any other medium.
- When publishing students' work, staff must take care to ensure that no personal information is revealed in the work that can be connected to a student.

2.3.5 Social networking and personal publishing

- School will block/filter access to social networking sites wherever possible.
- Newsgroups will be blocked, where possible, if they contain inappropriate material.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students will be advised not to place inappropriate photos or personal details on any social network space and made aware of the security implications of this.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

2.3.6 Managing filtering

While the school makes every effort to protect students from unsuitable materials, due to the international scale and connected nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer. Filtering is carried out by both the LEA and the school

- The school will work in partnership with the Local Authority, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The use of “proxy sites” to bypass school or LEA filters is prohibited and the school will endeavour to block these sites where possible.

2.3.7 Managing videoconferencing and filming/photography

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students’ age.
- Parents and guardians should agree for their children to take part in videoconferences, filming or photography, in the annual data collection sheet at the start of the academic year.

- Personal recording equipment, cameras and mobile phones must not be used in school without permission from the class teacher.

2.3.8 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.
- Mobile phones of students in Years 7,8 9, 10 and 11 must be out of sight and switched off and not be used during lessons or formal school time unless a teacher gives permission for a phone to be used for a specific task. Post 16 students may use their phones in school in accordance with the AUP.
- Staff should avoid giving their mobile phone number to parents or students .
- In exceptional circumstances, such as school trips, staff can ask the school to provide a mobile phone and/or SIM card for use.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff and students must read and agree to the 'Acceptable use policy' before using any school ICT resource.
- The AUP and its implications will be explained to students.
- Students with Special Educational Needs will be given additional support in appreciating the requirements of the AUP.
- The school will maintain a current record of all staff and students who are granted access to school ICT systems.

2.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the 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.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a member of the senior leadership team.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of the complaints procedure.

2.4.4 Community use of the Internet

The school will liaise with local organisations (including adult and youth education) to establish a common approach to e-safety when using school systems.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to students

- e-safety guidelines will be shared during annual assemblies.
- Students will be informed that email, network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues. Internet issues will be handled sensitively and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. Guidance and suggestions will be provided for safe home Internet use.
- Guidance will include advice on filtering systems and educational and leisure activities that include responsible use.