E-Safety Policy

Reviewed Aug 2022

The purpose of this policy is to fully recognise the responsibility PCHS has to ensure e-safety for all. It supports the principle that e-safety is everybody's business.

This policy applies to all users of ICT at Prudhoe Community High School (PCHS), including but not limited to, staff, students and visitors. The policy also applies to the use of PCHS equipment taken off the school site with the permission of the Headteacher for educational purposes eg: laptops provided by the school to staff. The purpose of this policy is to ensure the safety of all people to whom it applies.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology as well as collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Northumberland County Council including the effective management of Lightspeed Filtering and Senso Monitoring Software.

School e-safety policy

- Our e-safety policy operates in conjunction with other policies including those for ICT, anti-bullying and for safeguarding and child protection and GDPR
- Our e-safety coordinator is John-Paul Nesbitt, Assistant Headteacher who is overseen by Faye Warkman, Acting Deputy Head and Designated Safeguarding lead (DSL).
- The e-safety policy and its implementation will be reviewed bi-annually unless there is a significant change in provision.

Role of e-safety officer

- Oversee the establishment and reviewing of the E-Safety policy, E-Safety Standard Operating Procedure, Social Networking Guidance and Acceptable Use Policy Documents
- Ensure any changes in Behaviour, Anti-Bullying, Data Protection and Safeguarding policies are reflected appropriately in the E-Safety Policy.
- Be a point of contact for Designated Child Protection Officers for safeguarding, offering support and advice in dealing with complex incidents and concerns
- Update the Headteacher and governing body about changes to the E-Safety policies, emergent technologies and a general overview of E-Safety on a regular basis.

Teaching and learning

Why Internet use is important

- The Internet is an essential element 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.
- Staff and Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning and benefit education:

- The school Internet access is designed for student use and includes filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use.
- The school will ensure that the use of Internet derived materials by staff and students complies with copyright law.

Managing Internet Access

- Information system security, School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- E-Safety Filtering is monitored and up to date.
- Web Filtering is monitored and up to date.

E-mail

- Students may only use approved messaging accounts on the school system.
- Students must immediately tell a teacher if they receive offensive messages.
- Students must not reveal personal details of themselves or others in e-communications, or arrange to meet anyone.
- E-communications sent to an external organisation should be written carefully and where necessary authorised before sending, in the same way as a letter written on school headed paper.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Staff should only use their @pchs.org.uk Google email address for professional communication and this should be the only way in which staff email students.

Published content and the school website

- The contact details on the Web site should be the school address, e-mail and telephone number.
- Student personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- Staff personal contact information will not be published. The contact details given online will be the school office and school contact details of selected key personnel only.

Publishing student images and work

- Photographs that include students will be selected carefully.
- Students' full names will not be used anywhere on the school website particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published by the school.
- Student work can only be published with the permission of the student and parents.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students and parents will be advised of the dangers of the use of social network spaces outside school.
- Students and parents will be advised the use of social network spaces outside of school will remain the responsibility of the students and parents.
- Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that parents and students may carry out web and social network service searches to find on-line information about staff, for example; background, interests, career experiences and self-presentation. All staff, perhaps especially new staff in training and induction, are advised to ensure that information available publicly about them is accurate and appropriate.
- Staff must not use internet or web-based communication channels, with the exception of their @pchs.org.uk Google email address and the school suite of Google Applications, to send personal messages to a child/young person, or their parents. This includes online gaming.
- Staff should not have any contact with students and should avoid contact with parents of students outside of their family network on a social networking website. If such contact is made, staff should be extra vigilant regarding the content of their posts to ensure they do not expose personal details which could be exploited, they do not breach student/parent/staff relationships and that they do not post anything which could bring the school into disrepute.
- Staff should not attempt to hide their identity online, for the purpose of contacting students, parents or others associated with the school, for example by using a pseudo name on a social networking site.
- Staff must not give their personal contact details to children or young people, including their parents.
- Staff should not identify themselves as working specifically for the school on social media.
- Staff are to understand that some of their communications may be called into question and may need to be justified.
- Staff are advised not to have online communications with ex-students whom have recently left the school and may have friends or family still within the school.
- Staff are strongly advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

Managing filtering

- The school will work with NCC, DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable website, it must be reported to any teacher who will report it to the e-safety coordinator who will in turn report it to the ICT Network Manager.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

- Video conferencing, where available, will be appropriately supervised for the students' age.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of mobile phones, smart watches and other internet enabled devices are prohibited except for use as authorised and directed by the teacher in charge of the student at the time. Such an authorisation is only valid for the period of the activity and does not constitute a blanket authorisation to use the device. The unauthorised use of cameras of any type is not permitted in school.
- Staff will be issued with a school phone where contact with students is required. Personal mobile

phone numbers will not be issued to students or parents.
- In the very rare occasion when a member of staff needs to use a personal device to contact a parent they should always make use of appropriate technology that withholds the number from the person they are contacting.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.
- All staff are required to use Google Drive or an encrypted memory pen for information storage.
- No files containing Personal Identifiable Information about anyone associated with PCHS should be stored on a computer not belonging to PCHS.
- Emails containing information about students and staff can only be sent through the @pchs.org.uk Google email system.

Staff Training

- All staff will be given the School e-Safety Policy and its importance explained. This will be done as part of the school induction process.
- All staff will complete child protection training every three years which will include a significant focus on E-Safety training
- Regular E-Safety messages will be delivered at the beginning of each term. This will be supplemented by announcements in weekly staff briefings for urgent or emerging issues.

ICT access

- All staff must read and sign the 'ICT Code of conduct' before using any school ICT resource.
- All students are asked to sign (and parents countersign) a copy of the 'ICT Code of Conduct'. A copy of the completed agreement is kept and only after this has been received will students be granted access to the ICT network.
- Post 16 students will be asked to sign an adult 'ICT Code of Conduct' to reflect the increased responsibility that they have to take as they get older.
- Everyone will be made aware that Internet traffic can be monitored and can be traced to an individual user.
- Students will be reminded of e-safety rules at the beginning of each year.
- Students will be informed that network and Internet use will be monitored in accordance with the student Code of Conduct.
- Parents' attention will be drawn to the School e-Safety Policy on the school Website. Any suitable e-safety resources that are produced for parents will be made available.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Northumberland County Council can accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with by a senior member of staff.

Responding to Incidents of Misuse

- Incidents and complaints of Internet misuse will be dealt with by the e-safety coordinator in conjunction with the Designated Safeguarding Lead or other member of the Senior Leadership Team.
- Any incident or complaint about a member of staff must be referred to the Headteacher and may be referred to the Local Authority Designated Officer (LADO).
- Incidents and complaints of a safeguarding nature must be dealt with in line with the school safeguarding and child protection procedures.
- The school will adopt the NCC procedures for dealing with E-Safety issues (see incident management flowchart).

Consequences

- In the case of student misuse the full range of school consequences may apply including exclusion.
- In the case of staff misuse disciplinary procedures may apply.

Cyber-bullying

- Cyber-bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school anti-bullying policy
- There will be clear procedures to support anyone affected by cyber-bullying.
- There will be clear procedures in place to investigate incidents or allegations of cyber-bullying. The police will be contacted if the school feel it is appropriate.
- Where Cyber-bullying takes place on social media or via massaging services the school will always advise parents/ carers to report this to the police as offences may have been committed and the police are the appropriate body to deal with such matters.

Use of mobile devices

- Where a mobile device is provided to an individual by the school this device is for the exclusive use of the person to whom it is provided and is for school business use only.
- Where users are permitted to access the school suite of Google Applications on their own or school devices they accept full responsibility for ensuring that the device requires a password or passcode to allow access. They should always be logged out so that no user can access school information.
- School devices are filtered and monitored when in school and accessing the school network and when being used away from the school site. However staff, students and parents also need to take responsibility for devices used outside of the school network and the school cannot be held responsible for usage outside of the school network, although may still issue consequences for inappropriate use that it is aware of as described earlier in this policy.
- School devices should only be used by school staff and not family members.
- Personal devices should utilise a secure log on and should only be used by the person currently logged on. Users should log out and secure the device whenever they have finished using it.
- Personal devices should have settings configured to ensure that email and other systems are secure in line with PCHS requirements, e.g. strong passwords to access each time, auto time out, auto screen lock, etc.
- The school cannot be held responsible for students accessing the internet using their own 3G/4G data connection on their own devices.

Monitoring of this policy

What?	**How?**	**When?**
eSafety Audit	eSafety Consultant	Annually
Review by governors		Bi-annually

Linked documents

Adult user agreement
Student user agreement
Remote learning strategy
Student code of conduct - Live lessons
Incident management flowchart

Action	By whom	By when
Updated	John-Paul Nesbitt - Deputy Head	January 2021
Approved	Rob Moore - Chair's Action	29 April 2016
Reviewed	Susan McArdle - Chair's Action	February 2020
Reviewed/approved	Susan McArdle - Chair's Action	27 January 2021
Reviewed	JPN	August 2022
Approved`	Chair's Action (SMC)	17/09/2022
To be reviewed	Leadership	August 2024