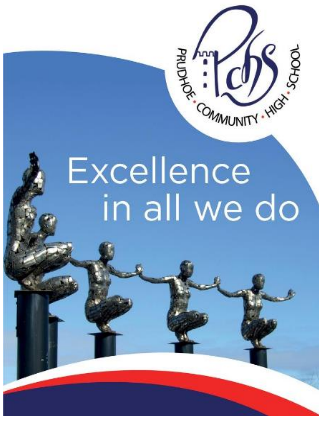

Name:

ICT Code of Conduct for Adult Users (updated Sept 2022)

The school has an E-Safety Policy drawn up to protect all parties - the students, the staff and the school. This code of conduct is for all adult users including students in the sixth form. It should be read in conjunction with the E-Safety Policy.

The computer system is owned by the school and is made available to Adult Learners to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system, and to track and/or monitor user activity or Internet sites visited. Neither the School, however, nor the service provider, can guarantee complete safety from inappropriate material.

Access should only be made via the authorised account and password that must **not** be made available to any other person. Any activity carried out by a given username is the responsibility of that user.

The security of the ICT system must not be compromised, whether owned by the school, by Northumberland County Council or any other organization or individual.

Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.

Users are responsible for all e-mail sent and for contacts made that may result in email being received. The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded. Posting anonymous messages and forwarding chain letters is forbidden. Copyright of materials and intellectual property rights must be respected. All Internet use should be appropriate to staff professional activity or to student's education. Users are also responsible for reporting any weaknesses that they find in the school system to a member of the Senior Leadership Team.

Use of school equipment issued to users

- Where equipment is issued to an individual eg: Laptop, i-Pad, the user that is issued with the equipment is responsible for ensuring the equipment is not used in a way which would breach either this code of conduct or the E-Safety Policy. This includes use away from the school site when using other network connections.
- Users who are issued with loan devices must bring their devices back into the school when requested for the purpose of security updates and patches.

Use of own equipment

- Where users use their own equipment to access the wireless network within PCHS they will be required to use their network username and password. Usage will be subject to the same filtering and monitoring as when using school equipment. The code of conduct applies to all devices accessing the network regardless of the ownership.

- Where users use their own equipment to access the school suite of Google applications they will be required to ensure that the devices are secure in line with PCHS requirements, e.g. passwords or passcodes to access each time, auto time out, auto screen lock, etc.

Please note that:

- Staff who access their @pchs.org.uk Google email account using their own personal electronic devices are responsible for the security of that device and the data contained within. Preventing unauthorised access to sensitive and confidential information is the sole responsibility of the member of staff using and accessing the device. They should also make every effort to prevent family or casual users accessing their emails which may contain sensitive, personal or confidential information. Once the information has been processed, if accessed off site, it should be stored on an encrypted memory pen and no copies should be stored on personal machines. (Password memory software must not be used as it would compromise security and enable unauthorised access).

- Where staff or students are given access to the school suite of Google applications via their personal mobile devices they agree that on leaving the organisation Prudhoe Community High School reserve the right to auto delete data from their personal devices in addition to deactivating their account to ensure the security of all data.

- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- Closed discussion groups can be useful but the use of public chat rooms is not allowed.

- The school has adopted a number of policies on good practice with ICT usage which can be referred to for further information. These include Anti-bullying, social media, GDPR and Data Protection and E-safety policies as well as the school's remote learning strategy.

- All the school computers carry anti-virus and security software designed to identify any abuse of the network. Students and visitors are welcome to use personal laptops on the network however these machines will also be subject to the same scrutiny as the school machines. Monitoring and filtering software is used to monitor any inappropriate use of the school system. Any inappropriate use that has been identified will be investigated and could result in a disciplinary action.

Consequences of breaching this code of conduct

- In the case of an adult student user breaching this code of conduct the full range of school consequences may apply including exclusion. The school may also need to involve other agencies such as the police in some cases.

- All instances of a breach of this code of conduct by staff will be referred to by the Headteacher and disciplinary procedures may apply. The school may also need to involve other agencies such as the police in some cases.

Adult Learners are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet, or store or distribute such materials and that they are subject to the LEA's recommended disciplinary procedures should they do so. **Child Protection Legislation applies at all times when accessing the Internet.**

Staff code of conduct for Live Lessons

Teachers and students have a shared responsibility to establish and maintain a positive and supportive online learning environment and therefore must:

- join the video call prior to the session and start to record the video call as soon as you join.
- keep the recording (this will automatically be emailed to you) for 30 days after the live lesson.
- treat any audio or video call as a live lesson environment with the same expectations of appropriate behaviour and interaction as in school
- be on time for virtual classes;
- turn off or silence mobile phones during live interactions;
- provide feedback to SLT about your experiences and any relevant suggestions
- report any incidents or poor behaviour through the usual channels
- video conference from an environment that is quiet, safe, public and free from distractions
- if your camera is on please blur your background
- make sure you clearly end the session and stay in the class until all students have left.
- Contact f.warkman@pchs.org.uk, a.moore@pchs.org.uk or g.boddy@pchs.org.uk if there are any safeguarding concerns during the live session. In addition staff should also follow school safeguarding procedures through the use of CPOMS

I have read the Acceptable Use Policy and agree to abide by it.

Name

Signed

Date