Appendix 11 – Student ICT Acceptable Use Policy No. 44b

Computing Facilities

Students are encouraged to make use of the school computing facilities for educational purposes. All students are expected to be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

Due to high demand for computer facilities at lunchtimes, use of computers at this time must be restricted to school work only. **Students must not be in ICT rooms after school unless supervised by a member of staff.**

Students can access the school's email by either visiting the school website or by going to https://mail.cchsg.com/owa. To access any resources, students must go to the school website and access these through SharePoint.

Logging On and Security

- Students are responsible for the protection of their own network logon accounts and must not divulge passwords to anyone.
- Students must not log on as someone else, nor use a computer which has been logged on by someone else. Students should also log off when leaving a workstation, even for a short time.
- Any attempts to access, corrupt or destroy others users data, or compromise the privacy of others in anyway, using any technology is unacceptable.
- Computer storage areas are accessible by ICT staff who may review your files, communications and computer usage to ensure that you are using the system responsibly.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Use of the Network and Computer Facilities

All users must take responsibility for their own use of new technologies, including BYOD devices, making sure they use the technology safely, responsibly and legally. It is not acceptable to knowingly:

- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence, distress or anxiety to any other student or member of the school community, or is bullying or harassing in nature, or material which infringes copyright, or material which is unlawful. This will result in action being taken, according to the School Behaviour Policy.
- Download or install programs to a school owned computer or a BYOD.
- Introduce a virus, or malicious code.
- Bypass network and systems security, breach technical safeguards or conceal network identities.
- Access another student's account.
- Gain access to an unauthorized area or system.

- Use any form of hacking or cracking software / system.
- Use any applications or services to bring the school or its members into disrepute.
- Engage in activities which damage resources, waste teaching or technical support time or use the network resources in such a way so as to diminish the service for other network users.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Students have a responsibility to report any known misuses of technology including the unacceptable behaviour of others.

Students have a duty to report failings in technical safeguards which may become apparent when using systems and services.

Students must not eat or drink in a designated computer room or near any computer equipment, including a BYOD.

Use of the Internet

Filtering software is used on the school network to prevent access to inappropriate internet sites, and to protect the computer systems. Students should be aware that the school logs all Internet use.

- The use of public chat rooms is not allowed.
- The use of social networking and video websites is not allowed unless used for educational purposes and approved by the class teacher and/or e-Safety Coordinator
- Students should not copy (plagiarise) and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.
- Students should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- Students must not reveal their own or another student's personal information such as name, address, telephone number, email address or school name over the internet.

(See e-Safety Policy if further clarification is required)

Use of Email

All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.

- Student email accounts are primarily for communication between students and teachers in relation to school work.
- Students are not allowed to use email during lessons without the teacher's permission.
- If a student receives an e-mail from an unknown person, or which is offensive or upsetting, the relevant teacher or a member of the ICT technical staff

should be contacted. Do not delete the email in question until the matter has been investigated.

- The sending / forwarding of chain e-mails are not allowed.
- The sending of a large number of multiple e-mails is acceptable only for good reason. Before doing so, the student must obtain permission from the e-learning coordinator or Network Manager.
- Students must not open attachments from senders they do not recognise, or that look suspicious.
- Students should periodically delete unwanted sent and received e-mails.
- Students may only use the e-mail accounts set up by the School. The use of e-mail facilities such as Hotmail and MSN instant messaging must only be used with permission from the e-learning coordinator or Network Manager.
- Students should not use their school email address for signing up to any online accounts, or share their email address with persons/organisations not associated with the school without permission from the e-learning coordinator or the IT Manager.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Use of Online/Distanced Learning programmes – Teams

When using an online learning platform such as Microsoft Teams, students at CCHSG should ensure that;

- Every Team should have 2 members of staff
- Students should ensure that they have permission from their parents to participate in live streaming of lessons at CCHSG. Their parents should have signed the Live streaming consent declaration. No permission - No live stream
- Students should follow the clear ground rules any particular Team (e.g. no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details).
- Students should not record, re-produce or re-distribute materials from the live stream, including taking screen shots. They will be removed from the Team immediately if found doing so and sanctioned using the school's Behaviour, Rewards and Sanctions Policy
- All members of the Team who participate in live streaming do so in a neutral area, (ie, not in a bedroom or bathroom). Microsoft Teams has the capability to blur or neutralise a background should the user wish.
- Members of the Team should not disclose personal information to anyone in the stream; such as their location, date of birth or phone number to anyone on the livestream, these should always be kept private. School-allocated email addresses are the only email addresses to be used. Usernames and passwords should never be shared.
- Team members do not have to be visible –audio participation only is also acceptable.

- All members of the Team are dressed appropriately (i.e. follows the schools normal non-uniform day dress code)
- Teams should not be used on a one to one basis between staff and students. Remote learning on a one to one basis is not appropriate.
- If students are concerned or suspicious about any activity on Teams, they should report it to their Year Leader.

Personal Laptops / Computers

Non BYOD devices for example personal laptops / computers and hand-held devices are only allowed in school with written permission from the Year Leader who will specify the times when they can be used. Connection to the schools network is only granted with permission from IT Manager following discussion with the Senior Leadership Team.

Use of Other Technology

Technology such as media rich phones, Personal Digital Assistants (PDA), tablets (including iPads), e-readers, memory cards, USB Storage devices and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with the e-Safety Policy and used only during the times specified to students. Mobile phones should be turned off at all times during the school day, including at break and lunch times, in accordance with School Behaviour, Rewards and Sanctions Policy. Year 12 and 13 students are allowed to use their mobile phone in the Sixth Form Common Room area only.

Privacy and Personal Protection

- Students must at all times respect the privacy of other students and members of staff; this includes not taking photographs, video or sound recordings.
- Students should not forward private messages without permission from the original sender.
- Students should not supply personal information about themselves or others, on any type of websites or within email.
- People you contact on the internet are not always who they seem, therefore, students must not attempt to arrange meetings with anyone met via a website or email.
- When using social media students must keep all information about school private; especially naming which school is attended.
- Students must not upload any pictures or videos taken in school or that show school uniform to <u>any</u> social media sites including Facebook, YouTube, Instagram, WhatsApp or Snapchat
- Students should realise that the school has a right to access personal folders on the Network and/or confiscate personal technologies such as mobile phones. Privacy will be respected unless unacceptable use is suspected.

Disciplinary Procedures
Violation of this ICT Acceptable Use Policy may result in a temporary or permanent ban on network use. Additional disciplinary action may be taken in line with the School Behaviour, Sanctions and Rewards Policy. Where appropriate, police may be involved or other legal action taken. (See e-Safety Policy for further details)

ICT Services
Any problems or faulty equipment should be reported to a teacher or ICT technician immediately. Students should not attempt to repair equipment themselves.

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understand the above and agree to uphold the standards outlined within these guidelines and the e-Safety Policy.

Student Name: _____ Signature: _____

Date: _____