Appendix 10 – Staff ICT Acceptable Use Policy No 44a

Computing Facilities

The school's network of computer systems and devices is owned by the school and is made available to staff in order to support their professional work. This ICT Acceptable Use Policy has been written to protect all users – students, staff and the school community. You are responsible for professional behaviour when using the systems, all of its resources and the Internet. You are expected to be an active participant in e-Safety education, taking personal responsibility for your own and your students' awareness of the opportunities and risks posed by new technologies.

This policy applies to using school resources both on-site and off-site. You agree and accept that any computer/laptop or other ICT device loaned to you by the school is provided solely to support your professional responsibilities and that you will notify the school of "any significant personal use" as defined by HM Revenue and Customs, and seek permission for such use from either Associate Principal.

Staff should refer to the full e-Safety Policy (No44) or e-Safety Coordinator for further clarification or details. It is the responsibility of employees to read the latest version of the policy because technology and the law change regularly.

Staff can access the school's internal systems from outside school by using the school provided devices (Laptops / Cloud books / Tablets) that have been enabled for use with Direct Access. These devices will work the same outside of the school as if on site with the only requirement being an internet connection.
If not using a school owned device then email can be access via the website or via:
https://mail.cchsg.com/owa
To access files that have been migrated to the cloud, these can be accessed through SharePoint, of which the link for this resources is found on the school website.

Logging on and Security

- You are responsible for the protection of your own network logon accounts and should not divulge passwords to anyone else.
- Always be wary about revealing your home address, telephone number, or school name on the Internet. Personal details of any adult working at the school or student at the school should not be given. (see e-Safety Policy)
- Other computer users should be respected and should not be harassed, harmed, offended or insulted. (See e-Safety policy)
- Always log off when leaving a workstation, even for a short time.
- To protect yourself and the systems, you should respect the security settings on the computers; attempting to bypass or alter the settings may put you or your work at risk. (See e-Safety policy)
- Computer storage areas are accessible by ICT Services IT Helpdesk staff who may review your files, communications and computer usage to ensure that you are using the system responsibly. (See e-Safety policy)

Use of the Network and Computer Facilities
All users must take responsibility for their own use of new technologies, making sure they use the technology safely, responsibly and legally. It is unacceptable to knowingly:

- Install any unauthorised software. Always get permission from the Network Administrator before installing, attempting to install or store programs of any type on the computers.
- Damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. This puts yours and others work at risk.
- Introduce a malicious code or virus. If using removable media such as USB memory sticks do not open any files that you suspect may have been infected with a virus or malicious program. The network anti-virus programme should notify you before infected files are opened.
- Try and gain access to an unauthorised area or system.
- Use any form of hacking or cracking software / system.
- Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence, anxiety or distress to other network users, or material which infringes copyright, or material which is unlawful.
- Use any applications or services to bring the school or its members into disrepute.

The network and computers are provided for professional and educational purposes. You may use the computers for private use in your own time providing that use does not prevent others from using resources for work purposes. (see e-Safety Policy for restrictions)

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

You should protect the computers from spillages by eating or drinking well away from the ICT equipment.

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. Staff should be aware that the school logs all Internet use.

Access to the Internet is provided for school activities. You may access the Internet for reasonable appropriate private use in your own time providing that use does not prevent others from using resources for work purposes. (See e-Safety policy for restrictions)

Connection to the schools wireless network is permitted only for professional/educational purposes only. Connection with personal devices such as tablets or smartphones permitted only at the discretion of the e-Safety Coordinator, Senior Leadership Team and Network Administrator.

Only access appropriate material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive or likely to cause anxiety or distress is not permitted. (See e-Safety Policy for definitions)

You should respect the work and ownership rights of people outside the school, as well as other staff or students. This includes abiding by copyright laws. (See e-Safety Policy Appendix 6 for details.)

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. Automated software scans all email, and removes anything which could affect the security of the computer systems, or contain unsuitable or offensive content.

Only the school email account should be used for emails which are sent on school business. You should not use a personal email account for school business. Remember that any emails sent using a school email account are sent on behalf of the school in the same way as official letters. Emails should be professional in language and tone and should not compromise the reputation of the school.

Your school email account should not be used routinely to communicate with family and close friends. Personal email accounts should be used for personal communication and also to sign up for mailing lists or online communities that are not school related.

Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, or which is bullying in nature, you should always report such messages to a member of ICT support staff and your line manager.

Emails should not be used during lessons unless it is deemed an emergency. Emails should not be used to communicate with colleagues on aspects that could be deemed of a personal or casual nature.

The sending of an email or text containing content likely to be unsuitable for students or schools is strictly forbidden.

You should regularly delete unwanted sent and received e-mails.

Social Media

The use of social media can enhance teaching and learning but is also used widely for social interaction. With this in mind, teachers should exercise extreme caution when using social media sites such as Facebook and ensure maximum privacy settings. (See e-Safety Policy for further guidance and clarification)

Under no circumstances should a teacher use a personal social media account in the classroom or to facilitate their lessons. It is unacceptable for a member of staff to accept a friend request from an existing student on a personal social media account. See 44c Social Media Policy for further guidance.

Use of Online/Distanced Learning programmes – Teams

When using an online learning platform like Microsoft Teams, staff at CCHSG should ensure that:

- Every Team should have 2 staff members to safeguard everyone in the Team, the additional person should ideally be a Head of Department or Year Leader
- Staff should ensure that students participating in a live stream has permission from their parents to be there. No permission - No live stream
- Staff and students should establish and follow clear ground rules of that particular Team (e.g. no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details). This is likened to a teacher creating the correct climate for learning in their classroom. If live streaming, these rules need to be reiterated every session
- 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 reported to the e-Safety Coordinator.
- All members of the Team participate in live streaming in 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 must never be shared.
- Team members do not have to be visible –audio participation or via live chat only are 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.

Personal Laptops / Computers / Devices

Personal laptops / computers / hand-held devices are only allowed to be used in school with permission of the Principal. Connection to the school network however must be agreed with the e-Safety Coordinator, Senior Leadership Team, Principal and IT Manager.

Disciplinary Procedures

If you breach these provisions, access to the network may be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff Code of Conduct and Disciplinary Procedures. Where appropriate, police may be involved or other legal action taken. (See e-Safety Policy for details).

ICT Services Helpdesk

Any problems or faulty equipment should be reported to the ICT Services IT Helpdesk immediately. You should not attempt to repair equipment yourself.

Mobile Device Encryption

To comply with the Data Protection Act 2018, all school owned mobile devices that could be used off site will be encrypted enabling us to ensure that all data will be kept secure if the device is lost or stolen. (A mobile device can be described as any portable device which can hold data on the local drive which would be accessible by other means if this device was lost or stolen.)
Encryption will be managed by ICT Services. No user other than a person in ICT Services may decrypt the drive on a temporary or permanent basis. Failing to adhere to this will make you liable for any data access breaches which could incur fines.

Remote Data Wipe

CCHSG staff who have access to school email through their mobile phones must accept that ICT Services will have the right to remote wipe the device to prevent any data access breaches if the device is lost or stolen. Failure to notify ICT Services in the event of a device being lost or stolen will render you personally liable for any fines incurred.

Privacy and Personal Protection

- CCHSG staff must at all times respect the privacy of other students and members of staff; this includes not taking photographs or video or sound recordings.
- Staff should not forward messages (private or otherwise) without permission from the original sender.
- Staff should not supply personal information about themselves or others, on any type of websites or within email.

- When using social media staff must keep all information about school private; especially naming the school which you work at.
- Staff must not upload any pictures or videos taken in school or that show school uniform to any social media sites including Facebook, YouTube, Instagram, WhatsApp or Snapchat

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.

Staff Name: ___________________ Signature: ________________Date: __________

Policy links: AT2 Safeguarding & Child Protection Policy A4
Behaviour, Sanctions & Rewards Policy
A5 Anti-bullying Policy
26 Code of Conduct
44c Social Media Policy

Reviewed February 2022