ICT Acceptable Usage Policy

Introduction
The purpose of this policy is to ensure that users of CTTC and the Colchester County High School for Girls' (CCHSG) ICT systems and services understand the way in which it is to be used. The policy aims to ensure that the ICT is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

Scope
The policy applies to:
All users and administrators of the CTTC and CCHSG services and/or infrastructure.

Policy Statement
This document should be read in conjunction with the **44 CCHSG E-Safety Policy including AUP** and **Code of Conduct**.

Please read this policy carefully as you will be deemed to be aware of its contents.

During school placements please ensure you obtain a copy of/and follow the school policy on the use of the Internet and online access. Whilst training with CTTC, Trainees will be bound by the following:

Computing Facilities
The school's network of computer systems and devices is owned by the school and is made available to trainees in order to support their professional work. This includes free access to wi-fi in the training rooms.

This ICT Acceptable Use Policy has been written to protect all users – students, trainees and the school community. You are responsible for maintaining professional behaviour when using school systems, resources and Wi-Fi. This Policy applies to the use of school ICT resources both on-site and off-site.

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.

Any computer, laptop or other ICT device loaned to you by the school is provided solely to support your professional responsibilities. Any personal use must be reasonable and incidental. Where personal use becomes significant, as defined by HM Revenue and Customs, you must notify the school and seek permission from the Headteacher.

Trainees should refer to the full E-Safety Policy or E-Safety Co-ordinator for further clarification or details.

Logging on and Security

- You are responsible for the protection of your own network logon accounts and should not divulge passwords to anyone else.
- Do not reveal your home address, telephone number, or details about the school or CTTC 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 lock or 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 staff who may review your files, communications and computer usage to ensure that you are using the system responsibly. (See e-Safety policy)
- Internet traffic through the system and Wi-Fi is monitored by ICT staff who will alert Directors of any inappropriate usage.
- Monitoring will be proportionate and in line with data protection legislation.

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.
- Attempt to gain access to an unauthorized 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 Artificial Intelligence (AI)

Artificial intelligence (AI) and automated digital tools may be used to support professional learning where their use is transparent, ethical, and compliant with CTTC requirements, school policies and academic regulations.

The use of AI must not compromise professional standards, academic integrity, safeguarding or data protection.

It is unacceptable to:

- Use AI tools to generate lesson plans, assignments, assessments, reflections, or evidence that are submitted as your own work without explicit permission or appropriate acknowledgement.
- Use AI to fabricate, falsify, embellish or misrepresent professional records, reflections, observation notes, assessment evidence or communications.
- Upload or input confidential, personal, or identifiable information relating to pupils, schools, staff, mentors or trainees into AI systems or online tools.
- Use AI to rewrite or disguise plagiarised material in order to evade academic integrity or plagiarism detection processes.
- Use AI to impersonate others, generate false correspondence, or misrepresent professional judgement or decision-making.
- Use AI to create content that is offensive, misleading, inappropriate, or likely to bring the school, CTTC, or the teaching profession into disrepute.

Any misuse of AI will be treated as a breach of this ICT Acceptable Use Policy and may result in disciplinary action in line with the Code of Conduct and academic regulations.

Work submitted for the PGCE qualification must follow the guidance set out by the University of Suffolk's General Regulations for Students guidance, which incorporates the Academic Misconduct Policy.

Both documents can be found here: General Regulations for Students Academic Misconduct Policy

Further guidance on using AI can be found on the University of Suffolk Library and Learning Services AI support hub here: Home - Artificial Intelligence - Learning and Teaching at University of Suffolk

Where there is any uncertainty about the acceptable use of AI, trainees must seek guidance from CTTC before using such tools.

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 school's 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, receive, create, copy, print, display, distribute 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.

A CTTC email account is provided to access CTTC systems, including Microsoft Teams and Outlook. Remember that any emails sent using a CTTC email account are sent on behalf of the CTTC in the same way as official letters. Emails should be professional in language and tone and should not compromise the reputation of the school. The content should be appropriate and accurate, and data protection compliant.

It is acceptable to use your CTTC email account in communications with family and close friends, but this privilege should not be abused. Personal email accounts should be used for wider personal communications and also to sign up for mailing lists or online communities that are not CTTC or school related. Emails must not be used to communicate with pupils except where explicitly authorised and recorded.

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 a CTTC Director.

The sending of an email or text containing content likely to be unsuitable for children 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. Trainees must exercise a high level of professional judgement when using social media platforms such as Facebook, X, TikTok and online gaming platforms. Trainees should ensure maximum privacy settings are used. All trainees are advised of setting their social media accounts to the maximum privacy settings at interview (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 Social Media Policy for further guidance). Trainees are explicitly prohibited from posting content that could identify pupils, schools or placements.

All trainees are advised at interview that Google checks will be conducted prior to the start of their training year, and regular Google searches may be conducted during the training year.

Personal Laptops/Computers/Devices
Personal laptops/computers/hand-held devices are only allowed to be used in school with permission of the Headteacher. Connection to the school network must be agreed with the e-Safety Coordinator, Senior Leadership Team and Network Administrator.

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 IT Helpdesk technician team immediately. You should not attempt to repair equipment yourself.

Mobile Device Encryption
To comply with Data Protection, 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.

Professional Boundaries Beyond Training
Whilst this policy applies during training with CTTC and within placement schools, trainees are reminded that their professional responsibilities extend beyond the duration of their training year.

As a professional expectation, trainees should not form online friendships or connections with former pupils until a minimum period of three years has elapsed from the point at which the trainee completed their training or last worked with the pupil in a professional capacity.

Trainees are expected to exercise sound professional judgement at all times and to maintain appropriate boundaries in line with safeguarding advice and the Teachers' Standards.

Privacy & Monitoring
The school does not routinely inspect individual communications but reserves the right to monitor usage of emails, data or the internet. Employees should therefore not expect absolute privacy in the use of school systems or equipment. Under certain circumstances the school reserves the right to review any electronic files and messages to the extent necessary to ensure systems are being used appropriately. Monitoring will be reasonable and in accordance with current legislation. See Code of Conduct.

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, the E-Safety Policy and Code of Conduct. This policy applies throughout the duration of your training with CTTC.

Trainee Name: _____ Signature: _____Date: _____

CCHSG Policy links:
A3 Safeguarding & Child Protection Policy
A4 Behaviour, Sanctions & Rewards Policy
A5 Anti-bullying Policy
26 Code of Conduct
44 E-Safety Policy
44c Social Media Policy

Ratified: December 2025
To be reviewed: December 2027