

ICT Acceptable Use Policies

For Students, Staff, Visitors

January 2019

CTC Students ICT Acceptable Use Policy

- I know that college computers and Internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed then I will ask a member of staff
- I know that my use of college computers/devices and Internet access will be monitored
- I will keep my password safe and private as my privacy, college work and safety must be protected
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present
- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment
- I will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the college community
- I understand that it may be a criminal offence or breach of the college policy to download or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18
- I will protect my personal information online at all times
- I will not access or change other people files, accounts or information
- I will only upload appropriate pictures or videos of others online and when I have permission
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I will always check that any information I use online is reliable and accurate
- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences
- I will only change the settings on the computer if a member of staff has allowed me to
- I know that use of the colleges computer system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the college's Internet filter is there to protect me, and I will not try to bypass it.
- I know that if the college suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow this ICT (Information & Communications Technology) policy then:
 - I may lose access to the college ICT equipment
 - Other appropriate disciplinary action as directed by the Senior Leadership Team
- If I am aware of anyone trying to misuse technology then I will report it to a member of staff
- I will speak to a member of staff I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers/hostess

Using CTC ICT equipment confirms that I have read and understood and agree to comply with the CTC Students ICT AUP (Information & Communications Technology Acceptable Use Policy)

CTC Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the college's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the college systems, they are asked to read and confirm compliance with this Acceptable Use Policy. This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the college ethos, other appropriate college policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, smartphones, tablets, email and social media sites.
2. College owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information.
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the IT support dept.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely. Any images or videos of students will only be used according to the appropriate college policies (contact SLT for clarification) and will always take into account parental consent.
7. I will not keep or access professional documents which contain college-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured / encrypted. Where possible I will use the College Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
8. Any stored personal information on the college computer system including any college laptop or similar device issued to members of staff that is unrelated to college activities, such as personal photographs, files or financial information must comply with all CTC policies.
9. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Patricia Brown). I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Head of IT (Winston Wong), and Designated Safeguarding Lead immediately in person.

10. I will not attempt to bypass any filtering and/or security systems put in place by the college. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any college related documents or files, then I will report this to the Head of IT immediately in person.

11. I will respect copyright and intellectual property rights.

12. My electronic communications with students, parents/carers and other professionals will only take place within clear and explicit professional boundaries. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership Team and/or Principal.

13. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the college AUP and the Law.

14. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or anxiety to any other person, or anything which could bring my professional role, the college, into disrepute.

15. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

16. If I have any queries or questions regarding safe and professional practise online either in college or off site, then I will raise them with the Designated Safeguarding Lead or the Principal.

17. I understand that my use of the college information systems (including any devices provided by the college), college Internet and college email may be monitored and recorded to ensure the safety of students and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The college may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the college information system or unacceptable or inappropriate behaviour may be taking place, the College will invoke its disciplinary procedure. If the college suspects that the college system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

Using CTC ICT equipment confirms that I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the college community are fully aware of the colleges boundaries and requirements when using the college Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the college community are reminded that ICT use should be consistent with the college ethos, other appropriate policies and the Law.

Please be aware that the college will not be liable for any damages or claims of any kind arising from the use of the wireless service. The college takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the college premises that is not the property of the college.

The college provides Wi-Fi for the college community and allows access for educational purposes.

1. The use of ICT devices falls under Cambridge Tutors College's Acceptable Use Policy, and behaviour policy, which all students/staff/visitors must agree to, and comply with.
2. The college reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
3. College owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
4. I will take all practical steps necessary to make sure that any equipment connected to the colleges service is adequately secure (such as up-to-date anti-virus software, systems updates).
5. The college's wireless service is not secure, and the college cannot guarantee the safety of traffic across it. Use of the college's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the college harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.
6. The college accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the college's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the college from any such damage.
7. The college accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the college's wireless service.
8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
9. I will not attempt to bypass any of the college security and filtering systems or download any unauthorised software or applications.

10. My use of the college Wi-Fi will be safe and responsible and will always be in accordance with the college Acceptable Use Policy and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material, which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything, which could bring the college into disrepute.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Patricia Brown) or the Principal immediately in person.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Designated Safeguarding Lead or the Principal.

14. I understand that my use of the colleges Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the colleges suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the college terminate or restrict usage. If the College suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

Connecting to the college Wi-Fi confirms that I have read and understood and agree to comply with Cambridge Tutors College Wi-Fi Acceptable Use Policy

Reviewed January 2019 CD

Reviewed August 2019 CD

Next Review August 2020