The Collegiate Trust
Exceptional Education for All

ICT POLICY

Lead	**Director of IT**
Reviewed by Staff	**Spring 2022**
Approved by TCT	**May 2022**
Full Review	**Spring 2024**

1. Aims and Objectives

The Collegiate Trust is a partnership of academies in Crawley and Croydon whose purpose is to build *collaboration to deliver exceptional education*, and whose vision is *exceptional education for all*. This is reflected in our Trust's values: **ambition** & **collaboration**, as well as in our desired outcomes: **achievement** & **enjoyment**. This policy outlines the control mechanisms around our key communications and management information system.

Our aim is that all members of the Trust are able to use ICT systems to support the operation of the Trust's schools and central teams with the purpose of providing high quality teaching and learning. As such, we shall ensure:

- Computer systems have effective security systems
- Data is protected
- Internet usage supports professional, lawful and ethical working practices

2. ICT Systems

The Collegiate Trust (TCT) provides computers for use by staff and students as an important tool for teaching, learning, and administration of TCT schools. Use of TCT IT systems, by all permitted users, is governed at all times by the following policy. Any questions or concerns should be discussed with the Director of IT in the first instance.

All staff and students have a responsibility to use TCT IT systems in a professional, lawful, and ethical manner. Deliberate abuse of TCT IT systems may result in disciplinary action (including possible termination or expulsion), and civil and/or criminal liability.

3. Computer Security and Data Protection

- Staff and students are provided with individual accounts to various IT systems. Accounts are tailored to the level of access required by that person. As such, account details must not be disclosed to anyone. Should staff require additional access appropriate to their role, they should contact their Line Manager or IT Support Team.
- Students must not use a staff account under any circumstances, for any length of time, even if supervised.
- Visitors must not be provided with access to staff accounts or areas. Appropriate guest accounts will be provided by ICT Support staff upon request. The school may additionally have a visitor wireless access system.
- Passwords must be kept secure, not easily guessable and not shared with anyone.
- The use of "Multi Factor Authentication" (MFA/2FA) is implemented for access to some systems for external access (when not on a school site). This requires the use of an 'Authenticator' app on a mobile phone. The Trust does not routinely provide this equipment. Therefore, staff not wishing or able to use MFA apps on their own personal device will not be able to access some systems remotely.
- When leaving a computer unattended, users must ensure they have logged off or locked (staff only) the computer to prevent anyone gaining unauthorised access.
- Sensitive or personally identifiable information about staff, students or administrative documents must not be stored on any portable storage system (such as a USB memory stick, portable hard disk,personal computer or personal cloud storage) unless that storage system is encrypted and explicitly approved for such use by TCT.
- Cloud Storage including, but not limited to Dropbox, personal Microsoft OneDrive, Google Drive and Apple iCloud services must not be used to store sensitive or personal information. TCT provides approved managed cloud storage services.
- Internet access is restricted and filtered to a level deemed appropriate for the relevant user. Sites are categorised, as 'allowed' or 'denied'. Some legitimate sites may be blocked. IT Support staff can investigate modifications required to Internet filtering, including reviewing and blocking inappropriate sites which are not already restricted
- Sending or sharing personally identifiable information, including audio and video files must be for authorised purposes with appropriate permission gained.
- Transmission of any sensitive or personal information via any electronic means must be encrypted using a method approved by TCT.
- The identity of students must be protected when publishing or transmitting non-sensitive material outside of any TCT school.

- Personal devices used for work purposes, must be kept secure to prevent any Trust related sensitive or personal information being accessed or stolen by any unauthorised party.
- Staff and students who use any storage system other than the TCT's network are responsible for ensuring adequate and secure backups of data are kept. IT Support staff are unable to assist with the recovery of files held on non-networked systems and users should note that files stored in Google Classroom, Google Drive, Microsoft OneDrive and Microsoft Teams is not routinely backed up; Therefore copies of important data should be saved on network drives as necessary
- IT equipment must not be moved or removed from the school without prior permission of Senior Management/Director of IT Some equipment is leased to the organisation and is not owned by the Trust.
- Portable items including laptops, digital cameras, and projectors must be securely stored when left unattended.
- Equipment taken offsite is not routinely insured by TCT. The borrower is responsible for any loss, damage or theft whilst the equipment is in their care.
- Access to CCTV and other monitoring systems is restricted to authorised staff and any footage or material gained from any Trust monitoring systems must be kept secure, for an appropriate length of time and only disclosed to relevant parties & authorities with consent from the Principal or Chief Operating Officer

4. Personal Use

TCT recognises that occasional personal use of Trust computers is beneficial both to the development of IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- must comply with all other conditions of this AUP as they apply to non-personal use, and all other Trust policies regarding staff conduct;
- must not interfere in any way with official duties or those of any other member of staff;
- must not have any undue effect on the performance of the computer system;
- must not be for any commercial purpose or gain unless explicitly authorised by TCT.

Access to your account will be revoked when you leave the organisation and cannot be kept for private purposes. It is your responsibility to back up any private messages or documents created within Trust systems before your last contracted day.

Personal use is permitted at the discretion of TCT and can be limited or revoked at any time.

5. Use of personal equipment

- Personal computer equipment must not be connected to any wired network socket or computer device without prior approval from the Director of IT. Except for storage devices such as USB memory sticks.
- Personal wireless devices may be connected to the appropriate BYOD wireless network where available.
- TCT cannot be held liable for any data or physical loss, damage or destruction of any personal device.

Personal computer equipment used to connect to any Trust system by way of the Internet or removable personal torage devices, must be protected by adequate anti-virus software and system security updates. Users must not connect from any device that may be infected or unsecure, nor attach any storage device that has been connected to an infected computer. Staff should not connect to Trust systems using public equipment as these may not be secure.

Access to any Trust system via public WiFi should only be made once the user has established a VPN connection to prevent unauthorised interception of passwords or private data. Any costs incurred for VPN services are at your own expense.

6. Conduct

- Use of all IT systems should be conducted professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Uses that are considered unacceptable (unless the curriculum requires them) include:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials; making ethnic, sexual-preference, or gender-related slurs or jokes.
- Security and access restrictions are in place to protect both individuals and TCT. All users must respect and not attempt to circumvent or disable restrictions.
- Intentional damage, disabling of, or otherwise harming the operation of any IT system is prohibited.
- IT resources must not be intentionally wasted. Examples include:
- Excessive downloading of material from the Internet;
- Excessive storage of unnecessary files on the network storage areas (e.g.: duplication, backups of USB sticks);
- Storing a large amount of personal files on systems;
- Use of desktop printers to produce class sets of materials, instead of using photocopiers;
- Leaving interactive screens or projectors on when areas are not in use.
- Eating or drinking around IT equipment should be avoided. Damage caused by accidental spillages may be chargeable.
- All use of the Internet is governed by TCT's Internet Acceptable Use Policy.
- Purchasing or entering in to a contractual agreement on behalf of the Trust or it's schools, without prior authorisation is prohibited. This includes:
    - Software titles and subscriptions;
    - Online services or resources;
    - Computer equipment.

  All software and online resources that require personally identified information such as names, email addresses, logins & class information must have a compliant Privacy Policy under the Data Protection Act. Before entering in to any trial or purchase, the Principal or COO and Director of IT must provide approval.

  Any equipment intended to directly or indirectly connect or attach to any Trust IT network or computing device must be authorised by the Director of IT prior to procurement. This includes devices such as:
    - Control technology;
    - Printers;
    - WiFi controlled devices such as thermostats, radiators and timers.

7. Supervision of Student Use

- Students must be supervised by staff at all times when using Trust IT equipment.
- When arranging use of computer facilities for students, staff must ensure supervision is available.
- Students must not, under any circumstances use a computer which is logged in with a staff account.

8. Privacy

- Use of TCT IT systems, including email accounts and storage areas provided for individual's use and may be subject to monitoring by TCT to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, TCT keeps complete records of sites visited on the Internet by all users. Usernames, passwords and financial information used on those sites are not monitored or recorded.
- Storage of sensitive personal information on Trust IT systems that are unrelated to educational activities (such as personal passwords, photographs, or financial information) should be avoided.
- TCT may use measures to audit use of IT systems for performance and diagnostic purposes.
- Use of Trust IT systems indicates consent to the above-described monitoring taking place.
- IT Support Staff may, with the permission of the Director of IT, access any user's area for support, diagnostic and security reasons.
- Staff must take care not to share or display sensitive data with others. For example, SIMS/Arbor or email messages shown on classroom displays/projectors.

- Phrase and screen loggers are implemented to detect inappropriate use of Trust IT systems and are reviewed by Safeguarding personnel, as required under the 'Keeping Children Safe in Education Act'.

9. Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook, Twitter & Instagram, even when such use occurs in their own time using their own device.

Staff must ensure that students cannot access personal information posted on a social networking site. In particular:

- Adding a student to 'friends' lists'.
- Ensuring personal information is not accessible via a 'Public' setting, by setting content to a 'Friends only' level of visibility.
- Not contacting any student privately via a social networking website, even for educational related purposes.
- Taking steps to ensure that any person engaging in electronic communication is whom they claim to be; i.e. not an imposter, before allowing them access to personal information.

Staff and students should take care when posting to any public website, including online discussion forums or blogs that comments do not harm their personal or professional standing or the reputation of TCT – even if their online activities are entirely unrelated to TCT.

Users must not:

- Unless authorised to do so, post content online which appears to represent the views of TCT.
- Post any material online that can be clearly linked to TCT which may damage TCT's reputation.
- Post any material clearly identifying individuals that could potentially be used to embarrass, harass, or defame the subject.
- Use images or videos of students without first checking for parental consent. All students are subject to parental authorisation for internal and external marketing purposes.

10. Internet Acceptable Use Policy

All users of IT systems must abide by this Acceptable Use Policy (which also applies when using a Trust device off site).

10.1 - Users must not:

- Attempt any method of bypassing the Trust's Internet filtering or firewall systems (e.g. 'Proxy Avoidance' sites or unauthorised VPNs).
- Download, install or run any program unless it has been authorised by the Director IT.
- Access any sites containing pornographic, immoral or offensive material or download/upload any such material or store it in your user area
- Send emails containing pornographic, immoral or offensive material.
- Enter into illegal or offensive activity, including the infringement of Intellectual Property Rights, copyright and UK laws.
- Use the Internet for personal gain, gambling or commercial purposes.
- Use the Internet for personal consumption during lesson or tutor times.

10.2 - Use of Electronic Communications

Members of staff who are provided with an email address and access to a telephone extension for communication both internally and externally should make the following considerations:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

- Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending.
- All e-mail messages sent by staff from a Trust account must have a signature containing their name, job title and the name of the school.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, users must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to TCT.
- Staff and students must only use authorised Trust systems to communicate electronically. Use of personal email accounts for communication is strictly prohibited.
- TCT takes measures to minimise the receipt and impact of unsolicited spam, phishing and malicious content, but cannot filter all such messages. Therefore, users must maintain caution before opening messages.
- Users must not send chain letters or unsolicited commercial e-mail.
- Use of any telephony system should be carried out in a professional manner and personal use kept to an absolute minimum.
- Data pertaining to use of any electronic system may be logged and reviewed by authorised managers. TCT may be required to disclose content and logs to external agencies as required for legal purposes.
- Electronic communication between staff and students must only be carried out using authorised Trust systems. Use of personal email accounts between staff and students should be avoided.

10.3 - Where available: Wireless Network/BYOD (Bring Your Own Device)

- All users must authenticate with their own credentials for monitoring and appropriate filtering and this should not be shared with others.All wireless traffic is filtered and logged.
- The use of the wireless network is not a right and prioritisation may be set to limit the impact to Trust IT systems. TCT reserves the right to withdraw, temporarily or permanently the use of wireless systems.
- In some schools, students may be permitted to use personal devices connected to the 'Bring Your Own Device' wireless network (where available) and should always authenticate with their own credentials for monitoring purposes. This is a requirement of the 'Keeping Children Safe in Education' policy.
- Visitors must not use staff or student accounts to access any wireless system. If a school has a wireless system in place, a guest pass should be issued to ensure appropriate access levels and monitoring are provided.
- Use of the wireless network is subject to same conditions as laid out above when using the wired network. It should be used in a professional, lawful, and ethical manner. Deliberate abuse of the system may result in disciplinary action (including possible termination or expulsion), and civil and / or criminal liability.

11. Confidentiality and Copyright

All staff and students are expected to:

- Respect the work and ownership rights of people outside of TCT, as well as other staff or students.
- Comply with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on Trust IT systems or the Internet are not marked with the copyright symbol (©), it should be assumed that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
- By storing or creating any personal documents or files on the TCT IT systems, all users of Trust systems grant TCT a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way TCT sees fit.

12. Reporting Problems with the Computer System/Peripheral Devices

It is the role of the Director of IT to ensure that TCT IT systems are working optimally at all times and that any faults are rectified as soon as possible. To this end:

- Staff should report any issues requiring attention through the correct channels (e.g.: the appropriate IT Helpdesk or Agency). Failure to report issues through the correct channels may lead to a delay in issues being resolved.
- If staff or students suspect equipment has been affected by a virus or other malware, it must reported to a member of IT Support staff immediately.

- Lost documents or files, should be reported as soon as possible. The retention period of backed-up data varies, therefore it is imperative that any restorative work is carried out at the earliest opportunity.

13. Reporting Breaches of this Policy

All members of staff have a duty to ensure this Policy is followed.
Staff must immediately inform a member of the IT Support staff, or their line manager (who must pass the information on to IT Support staff) of abuse of any part of IT systems.

In particular:

- any websites accessible on Trust IT systems that may be unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by any person via Trust IT systems.

14. Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities, significant changes to the organisation or technical infrastructure, changes to any applicable UK legislation. Changes to this policy will be communicated to all staff.

15. Sanctions

Employees breaching this policy will be referred to the Staff Disciplinary Policy.

Notes

"Sensitive personal information" is defined as information about an individual that is protected by law under the UK Data Protection Act. Examples of such data include addresses and contact details of individuals, dates of birth, and student SEN data. This list is not exhaustive. Further information can be found in TCT's Data Protection Policy.

Relevant laws, including the Computer Misuse Act, Data Protection Act, Copyright, Design & Patents Act and The Telecommunications Act apply to all users of Trust IT Systems at all times.