The Collegiate Trust
Exceptional Education for All

IT POLICY

Lead	**Director of IT**
Reviewed by Staff	**Spring 2024**
Approved by TCT	**June 2024**
Full Review	**Spring 2026**

1. Aims and Objectives

The Collegiate Trust is a partnership of schools 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. IT Systems

The Collegiate Trust (TCT) provides IT services and equipment 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.

The Trust uses security settings and software to ensure access rights & levels are appropriate. This does not guarantee that inappropriate materials may not be accessible, particularly with on-line services, nor does it provide automatic protection from security threats and hazards.

The Director of IT may delegate specific responsibility for maintaining systems & data integrity to other senior members of the IT Support Team.

3. Computer Security, System Integrity 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 or shared with anyone.
- Staff requiring additional access appropriate to their role should contact their Line Manager or Principal* for approval and submit a change request to the IT Support Team.
- Managers of new staff, including trainees, who require IT access, should make a request to IT Support in writing in advance of their start date. This should include access requirements.
- Managers of staff leavers or those changing roles should inform IT Support in writing of their final contracted date or changes, so access can be revoked or modified at the appropriate time.
- Students must not use a staff account under any circumstances, for any length of time, even if supervised.
- Visitors and volunteers must not be provided with access to staff accounts or areas. Appropriate guest accounts will be provided by IT Support staff upon advanced request. The school may additionally have a visitor wireless access system.
- Passwords must be kept secure, not easily guessable, nor shared with anyone.
- The use of "Multi Factor Authentication" (MFA/2FA) is implemented for access to some systems. This requires the use of an 'Authenticator' app on a mobile phone. The Trust does not routinely provide this equipment. Therefore, staff who do not wish or who are unable to use MFA apps on their own personal device will not be able to access some systems externally. MFA apps provide a 'key' to systems, but does not mean data will be available on the personal device.
- 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, fully updated with security patches and have robust & operational anti-virus/malware software and a firewall enabled to prevent any Trust related sensitive or personal information being accessed or stolen by any unauthorised party. Staff must not save credentials or sensitive information on a shared personal device, even within their own household.
- Data stored in network drives on school computers and the Trust's Microsoft 365 service, which includes Teams, OneDrive and Email, are backed up. Files stored elsewhere, including Google Drive & Classroom are not backed up; Therefore copies of important data should be saved elsewhere.
- 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. The Trust has a separate detailed CCTV Policy, available on our website.
- Special specific accounts must be used by students in place of their usual logins for time-based assessments and examinations. These will be created by IT Support. Staff must provide reasonable notice & specific restriction requirements in advance.

4. Equipment

- Trust owned or leased equipment is provided to support education and administration across the organisation.
- IT equipment must not be moved within or removed from the school without prior permission of Senior Management/Director of IT/Systems Administrators. Some equipment is leased to the organisation and is not legally owned by the Trust. IT Support must be made aware of any changes to accurately maintain equipment registers.
- Portable items including laptops, digital cameras & visualisers 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.
- Deliberate damage through poor behaviour or negligence, loss or theft by any staff or student may be chargeable to the involved party.
- Avoidable accidental damage may incur a financial contribution in part or full, at the discretion of the Principal / CEO.

5. 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 relevant laws and other conditions of this policy 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 any IT system;
- must not be for any commercial purpose or gain unless explicitly authorised by TCT.

Access to accounts will be revoked when the holder leaves the organisation and cannot be kept for private purposes, nor accessed beyond a contracted end date.

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

6. 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.
- Where available, authorised staff & students may connect a personal device to a "Bring Your Own Device (BYOD)" WiFi network.
- 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 must be protected by adequate anti-virus/malware software, fully up to date with system security updates and have a working & enabled firewall. 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.
- The Trust does not guarantee the availability of service for personal device or usage.
- Access to any Trust system via public WiFi should only be made once the user has established a trusted VPN connection to prevent unauthorised interception of passwords or private data. Any costs incurred for access or VPN services are not covered by the Trust.
- Personally identifiable information, including photos should not be used, stored or transmitted via personal devices.

7. Conduct

- Use of all IT systems should be conducted professionally, which includes being polite and acting in a safe, legal and business appropriate manner. In addition to the below, no behaviour which could contravene the Trust's Equalities Policy can be condoned. Uses that are considered unacceptable include:
  - Using, transmitting, or seeking illegal, 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;
  - Not attempting to circumvent, disable or remove restrictions and security settings, which are in place to protect individuals, the organisation and systems integrity ;
  - Intentionally damaging, disabling, 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.

8. Procurement

- Purchasing or entering in to a contractual agreement on behalf of the Trust or any of its schools, without prior authorisation is prohibited. This includes:
    - Software titles and subscriptions;
    - Online services or resources;
    - Computer equipment.

- Any software, online resource or service that requires personally identified information such as names, email addresses, logins & class information must have a compliant Privacy Policy under the Data Protection Act. It may be necessary to undertake a Data Protection Impact Assessment (DPIA) before authorisation can be granted. Staff should provide all relevant details and justification to the Data Protection Officer (DPO) before sharing any data.

- Staff must seek approval from ALL of the following parties before continuing with ANY agreement or purchase of software or online services;
    - Principal (or CEO)
    - Director of IT
    - Data Protection Officer (only where personally identifiable information is involved).

- Any procurement of 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:
    - Computing devices such as PCs, laptops and tablets;
    - Control technology;
    - Printers;
    - Peripherals such as visualisers;
    - WiFi or ethernet controlled devices such as thermostats, radiators, timers, sensors and alarm systems.

- Purchases against the IT Budget will only be authorised by the Director of IT in agreement with the Principal, CFO or CEO. Purchases from any other budget must be authorised by the relevant budget holder and will additionally require approval from the Director of IT.

9. 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 even when supervised.

10. Privacy

- Use of the Trust's IT systems, including Trust provided equipment used within or outside of any school, email accounts and storage areas, may be subject to monitoring by TCT to ensure compliance with this Acceptable Use Policy and applicable laws & statutory guidance, including 'Keeping Children Safe in Education'. This may include remote monitoring of an interactive logon session.
- Content generated or accessed on Trust computers may be automatically monitored for safeguarding purposes. Potential risks and breaches will be made accessible to the Director of Safeguarding, relevant DSL, Principal and CEO as appropriate and additionally, will be accessible to the Director of IT and System Administrators (who have signed a confidentiality agreement) where required. Information may be logged by a DSL in to external safeguarding record keeping systems such as CPOMS.

- The Trust retains data stored on network and Microsoft 365 systems, even after it has been deleted from active systems, for up to 7 years for compliance and legal purposes. This includes emails, files on network drives, OneDrive, Teams, SharePoint and messages. Data stored in compliance and offline backups is not intended to provide routine access.
- TCT keeps records of Internet activity by all users. Usernames, passwords and financial information used on sites is 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 and may be retained as part of routine backup & compliance policies.
- TCT may use measures to audit use of IT systems for performance and diagnostic purposes.
- IT Support Staff may, with the permission of the account holder, senior manager or Director of IT, or as part of their technical IT System Management duties, access any user's area for support, diagnostic or security reasons, but will not access file contents without prior consent.
- The Director of IT will provide access to any data held upon request from Principals or the CEO where any such request is reasonable & permissible under law.
- Staff must take care not to share or display sensitive data with others. For example, any information held in SIMS/Arbor or email messages shown on classroom displays/projectors.
- When using video conferencing facilities, which must be via authorised systems, staff and students should blur their background, be appropriately dressed and act in a professional manner.
- Students must not take still images or record audio or video during lessons without explicit consent of the teacher.
- Students must not share content with 3rd parties, without consent from their teacher or tutor.
- The monitoring and filtering systems are reviewed annually by the Director of IT as required by KCSiE and referenced to in the TCT Safeguarding Policy.

Use of Trust IT systems indicates consent to the above-described monitoring taking place.

11. Printing and copying

- Staff must use their own account with 'Follow-Me' / 'Hold-Release' printing queues to securely release jobs on designated copiers / printers.
- Sharing of printing credentials is not permitted.
- Staff may only print to an unauthenticated printer when it is situated in the same location (e.g. office or work area) and fully supervised. Permission will not be given to print to unauthenticated devices in another location, for any purpose.
- Staff should use Multi-Function or Professional level copiers for mass production, including whole class resources wherever possible. Desktop printers are usually more expensive to operate and are intended for low usage only.
- Care should be taken to check job settings are correct before printing and for complex jobs a test run should be carried out, to prevent accidental wastage and costs.
- Resources should be printed in mono unless there is a specific need for colour, to reduce costs.
- Deliberate wastage should be avoided.
- Printing and copying should relate to school purposes only. Personal use without prior permission from the relevant budget holder is prohibited.
- All printing and copying jobs are logged.
- All staff & student printing is charged to a specific budget. Access to budgets is granted by IT Support, who will require confirmation of authorisation from the relevant budget holder. Budget holders must request any top-ups or financial restrictions directly with the Finance Team.

12. Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook, X & Instagram, even when such use occurs in their own time &/or 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 a 'friends' list', following a student's profile or allowing a student to follow a private account.
- 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 any social networking or dating website or app, 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 the Trust.

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. Where consent is withdrawn, content must be withdrawn at the earliest opportunity.

13. Use of AI

- Artificial Intelligence services are usually processed on 3rd party systems externally. The Data Protection Policy applies when sharing any sensitive information with such systems. Therefore, staff and students must not share sensitive, private or personal information with AI systems as it is not possible to know who will see, store or re-publish this data. Examples include student results, reports, names & addresses, contact information, contracts, behaviour information, sanctions, communications with others that contain sensitive information, etc. AI systems are often hosted outside of the UK. The terms and conditions of many AI sites state that information may be re-used to train systems, may not be secure and could be re-published.
- You must not use AI to produce work and claim credit for the material.
- You must not use AI or other online resources to create, modify or share any material which may cause harm, offence or damage to any person or entity.
- You should be aware that AI may modify or generate material which contains bias, fake, false, inaccurate or offensive content. You should always fact check any results with other sources.

14. 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).

14.1 - 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.
- Transmit, access or store material containing illegal, pornographic, immoral or offensive material

- Transmit content or carry out any activity that may negatively impact a persons' personal or professional standing or physical & mental wellbeing, or harm the organisation.
- 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 outside of allocated breaks.

14.2 - Use of Electronic Communications

Members of staff and students in secondary schools are usually provided with a school or Trust email address. Most staff are provided with a '3CX' telephone extension for communication both internally and externally.

All users of Trust provided electronic communication services, should make the following considerations:

- Staff must undertake annual Cyber Security training as directed by the Director of IT and be aware of potential risks that could cause harm, including financial, personal, organisational, data integrity and system security.
- 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.
- Trust email accounts are provided for organisational purposes. Personal use, including subscriptions, purchases and communications should be avoided.
- 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 or other services 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 e-mail.
- Use of any telephony system should be carried out in a professional manner and personal use kept to an absolute minimum. All internal and external telephone calls are logged.
- 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 must be avoided.

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

- All users must authenticate with their own credentials for monitoring and appropriate filtering and this must not be shared in any way 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, some students may be permitted to use personal devices connected to the 'Bring Your Own Device' wireless network (where available) and must always authenticate with their own credentials for monitoring purposes. This is a requirement of the 'Keeping Children Safe in Education' policy.
- Visitors and volunteers 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.

15. 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 with the materials to use them.
- By storing or creating any resources or files on TCT IT systems, users grant the Trust 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.
- Note that online streaming services for audio and video usually prohibits public performance, including within schools. Care should be taken to understand and adhere to a sites' Terms and Conditions.

16. 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.

- Staff should report any issues requiring attention through the correct channels (e.g.: the appropriate IT Helpdesk). Failure to report issues through the correct channels may lead to a delay in issues being resolved. Staff should avoid emailing individual IT Support staff directly, unless otherwise instructed.
- If staff or students suspect equipment or accounts have been affected by a virus, malware, hacking, phishing or unauthorised access 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. Data Compliance policies are not a replacement for regular backup systems.
- Any unauthorised access must be reported to IT Support immediately.
- Staff must report loss or failure of, damage or vandalism to equipment to IT Support at the earliest opportunity and not assume someone else has already. IT Support personnel do not carry out routine inspections of all computing equipment.

17. 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.

18. 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.

19. Sanctions

Employees breaching this policy will be referred to the Staff Disciplinary Policy. Authorities may be involved in any case where there is suspected civil and / or criminal liability.

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.

* "Principal" includes any Head of School, Executive Principal and CEO.

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