Technology Policies and Procedures

2023-2024 Manual

TABLE OF CONTENTS

USE OF TECHNOLOGY

The following document aims to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Each school year, students, their parents/guardians, and employees must agree to all policies in this manual to utilize the TCA network, technology resources, and all technology-related items that belong to the school.

This privilege and extraordinary opportunity to explore digital resources come with responsibilities for each student and their parents/guardians. TCA will ensure that all students use technology and have access to it as an integral part of their learning experiences. In addition to the efforts of parents/guardians, TCA will adhere to its policies to maintain an environment that encourages ethical and responsible behavior in all electronic resource activities and uses.

STUDENT ACCESSIBILITY

PERSONAL DEVICES

Mobile Device/Phones/Smart/Bluetooth Policy for Students

- Students in the Secondary Department may bring mobile devices to the school campus for personal use after 3:00 pm.
- Students in the Elementary and Primary Departments are not permitted to possess mobile devices on school grounds at any time *(see 4.07.1 in the Family Handbook for more information).*
- Before school hours, mobile devices are to be powered off and stored out of sight.
- During school hours, mobile devices are to be powered off and stored in the owner's assigned locker or designated locking storage.
- Students may use their mobile devices during school hours only with the express permission and supervision of a Tacoma Christian Academy staff or faculty member (including the time between dismissal and 3pm).
- Students may use their mobile devices freely after 3:00 pm; however, if a student is discovered, at any time, using a mobile device in a manner that is not consistent with the school's mission,

values, or policies, the student will be considered noncompliant and the device will be confiscated and other disciplinary measures may be taken at the discretion of administration.

- Personal devices (i.e., laptops outside of the TCA approved devices scope, phones, tablets, or any other device capable of connecting to a wireless connection) are not allowed to be brought to school and/or connected to a student TCA network unless permitted by the IT Director and Principal.

- Students may not use external measures (i.e., a tablet with shared texting capabilities or other software that allows texting communication with SMS capabilities) to send Short Message Service messages (SMS), VoIP calls, or other messages including, but not limited to, iMessage, Google Hangouts, Slack, Jabber, Yammer, and QQ. Any student discovered using these services in class will be disciplined, outlined in the Violations and Discipline section.

- For the safety of all, use of the earbuds/airpods is permitted only when issued in writing by the Principal.

Failure to Comply

If a student is found hiding a cell phone or other mobile device between the hours of 7:30 am and 3:00 pm, the device will be confiscated and turned into the office. The student's parent or guardian will be notified and the student or parent may collect the phone from the office after school.

A fine will be charged for elementary and secondary students who fail to comply with the above policy.

Grade	Fine amount	Subsequent failure
Elementary students	$10.00/per violation	Increases by $5.00
Secondary students	$50.00/per violation	Increases by $10.00

Parents/guardians of primary students who habitually fail to comply with the above policy may have their fine increase rate moved to $10.00, rather than $5.00, at the discretion of the office, per violation. Students with repeated violations or those misusing/vandalizing technology may warrant a permanent ban on using cell phones, emails, and other electronic devices while being on school grounds.

Disclaimer

Tacoma Christian Academy (TCA) permits the possession of mobile devices by Secondary Department students out of consideration of the convenience of parents. While TCA will make every effort to ensure the security of mobile devices, TCA is not responsible for lost, stolen, or damaged devices. By voluntarily sending a student to school with a mobile device, parents/guardians release TCA of all liability related to said mobile devices without exception.

SCHOOL-PROVIDED DEVICES AND ACCOUNTS

1. Logging into a Device

- The student will log into their Devices using their school-issued account.
- The student will never share account passwords with other students.

2. Managing and Saving Digital Work

- Most student work will be stored in Internet/cloud-based applications and accessed from any computer with an Internet connection and most mobile Internet devices.
- The student should never forget to save often when working on digital media. Unfortunately, not all applications have an auto-save function.
- The school is/will not be responsible for the loss of any student work.

3. Listening to Music

- Any dev
- ice or personal device's sound must be muted at all times unless permission is obtained from a teacher.
- Headphones may be used at the discretion of the teachers.

4. Watching Movies/TV Shows/Digital Media

- Watching movies, TV shows or any other digital media on devices is not allowed during school hours unless permission from the teacher has been provided to complete a school assignment.

5. Webcams

- Webcams are to be used for educational purposes only, as determined under the direction of a teacher.

6. Gaming

- Online gaming is not allowed during school hours.

7. Backgrounds, Themes, and Profile Pictures

- Inappropriate media may not be used as backgrounds, themes, or school account profile pictures. The presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang-related symbols, or any other content deemed inappropriate by the administration will result in disciplinary actions.

8. Printing

- Students will be encouraged to publish and share their work digitally with their teachers and peers when appropriate.

- Students are expected to print all homework at home. Printing at TCA will be available for school-related assignments if a home printer is unavailable.

9. Chrome Web Store

- Students are not allowed to install approved Chrome Web Apps and Extensions from the Chrome Web Store.
- The downloading or manually installing (also side loading) of inappropriate material will result in disciplinary action.

10. Removable Media

- Removable media can be defined as, but not limited to, CD, DVD, USB devices, camera flash media cards, and hard drives physically removed from their laptops or computer-based machines.
- TCA reserves the right to pre-scan any removable media brought into the TCA network to ensure that it is free of viruses and other unwanted malware and spyware. Any individual who uses removable media must exercise extreme caution regarding the safe handling and security of the removable device and its contents.

12. Content Filter

- TCA utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA).
- Content filtering blocks most unwanted content and continues refining the algorithm it uses to improve protection.

13. Email Use

- An TCA email account is provided for all students through G Suite for Education. Email that originates from or is received by a school-owned computer or its contracted hosting company is the property of Tacoma Christian Academy and can be used during a legal proceeding.
- Use of this account is a privilege and can be revoked at any time.
- Use of email accounts by students will align with the Student Handbook code of conduct, and the code will be used for discipline purposes.
- Students who use TCA-assigned accounts, including the school-provided Google Account, are expected to exhibit maturity and common sense.
- Students are responsible for messages sent from their accounts. Therefore, students should exercise extreme caution with their passwords and never let a fellow student use their accounts.
- Students will not identify their home telephone numbers, home addresses, or any personal information in any email correspondence.
- Several student accounts are web-based and can be accessed outside the boundaries of our school; students are expected to maintain the same behavior that is expected of them while in school.

The following restrictions have been set for email accounts for all students: emails are allowed only inside of the TCA domain.

- In the event a parent and/or guardian would like to email their student using their TCA-provided email account, a special request should be submitted to the principal to allow cross-communication.

Exceptions to any of these policies may be made to support educational efforts as needed. Any attempt to avoid or violate any of the responsibilities outlined in this section will result in disciplinary action.

DEVICES

STUDENT RESPONSIBILITIES

The guidelines are offered here so that both students and parents/guardians are aware of the obligations that students undertake when they use a device that is owned by the school (referred to as a "Device" here). Devices include but are not limited to Chromebooks, iPads, laptops, smartboards, TV screens, photo and video cameras and audio equipment.

Utilizing all digital and informational resources effectively, responsibly, and legally is required while using technology. Violations of these rules and guidelines will result in disciplinary action.

The student will be responsible for:

- Carrying Devices in a Safe and Secure Manner.
- Transporting Device with care and with the screen closed.
- Never lifting Device by the screen.
- When not in the student's possession, Device(s) and its accessories are required to be placed in a secure location.
- Devices are not allowed in the lunchroom when food or drink is being served.
- Never setting books or stacking heavy objects on top of the Device.
- Never setting food or drink next to Device.
- Always carefully insert cords and removable storage devices into the Device.
- Always returning the device to its designated storage location (Chromecart or the IT Room.)
- Never defacing the device and its accessories by writing, drawing, coloring, stickers, etc.
- Never removing any logo, branding, serial numbers, stickers, or other ID tags on the device.
- Never storing a Device with the screen open.
- Always making sure there is nothing on the keyboard before closing the lid.

The student is accountable for the following:

- The student will never attempt to repair or reconfigure any Device.

- The student will not attempt to open or tamper with the Device's internal components, nor will the student remove any screws; doing so will void the manufacturer's warranty.
- Students will not damage their Devices intentionally.
- Students who take a Device home are responsible for returning it at the stated time.

Device Damage Reporting

If a student-assigned Device is not functioning correctly, is physically damaged, or otherwise, the student must report the findings to the teacher/instructor or take the device to the IT Room.

Checkout Guidelines

When a device or accessory is checked out from the IT Room, the following guidelines apply:

- Secondary students in grades 9-10 can check out a device during school hours.
- Secondary students in grades 6-8 must obtain permission from their teacher before checking out a device from the IT Room.
- The temporary loan of a TCA device must be returned to the IT Room no later than 3:00 p.m. on the same day.

PARENT/GUARDIAN RESPONSIBILITIES

1. Sign the Student/Parent Technology Agreement
2. Support Internet Safety Etiquette

Internet safety is about helping your child use the Internet productively and practice safe, responsible online behavior. The following are a few basic guidelines to share with your child:

- Follow your family's rules about when and where to use the Internet.
- Be polite, kind, and respectful in all Internet communications and whenever accessing technology.
- Understand a website's rules and terms and know how to flag other users for misbehavior.
- Recognize "red flags," including someone asking personal questions such as your name and address. Encourage your child never to share his or her name, the school's name, his or her age, his or her phone number, or his or her email or home address with strangers.
- Never send pictures to strangers.
- Keep passwords private (except from parents).
- Never open a message, link, or picture from any unknown source; it may contain a virus that can harm a computer.
- Immediately tell an adult if something makes you feel uncomfortable or something suspicious happens.

EMPLOYEE RESPONSIBILITIES

In additional to all standards and responsibilities in this handbook for parents and students, TCA employees are expected to:

- Change passwords according to school policy.
- Do not insert passwords into e-mail or other communications.
- Do not store passwords in a file without encryption.
- Utilize Google Drive storage for all files.
- Not store anything on the local drive or desktop.
- Never share ID/password for anything.
- Always lock devices when leaving them unattended.

Employees are responsible for any device issued to them. This includes laptops, Chromebooks, iPads, walkie-talkies, etc.

TECHNOLOGY AND COMMUNICATION

USE OF THE INTERNET

The question of Internet safety includes issues regarding the use of the Internet, and other electronic devices in a manner that promotes safe online activity for children, protects children from cybercrimes, including crimes by online predators and cyberbullying, and helps parents shield their children from materials that are inappropriate for minors.

To promote the safe and appropriate online behavior of students and staff as they access material from the Internet, the school will use the following four-part approach. However, given the ever-changing nature of the Internet, the school cannot guarantee that a student will never be able to access objectionable material.

1. Student/Parent Technology Use Agreement

Any student or staff member using the Internet from a computer in the school facility must have a valid Technology Use Agreement on file.

2. Filter

TCA utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). Content filtering blocks most unwanted content and continues refining the algorithm it uses to improve protection.

3. Supervision

When students use the Internet from school facilities, school staff will make a reasonable effort to supervise student access and use of the Internet. If material is accessed that violates standards in the materials selection procedures of the Technology Use Agreement, then school staff may instruct the person to cease using that material and/or implement sanctions contained in the TCA Technology Policies and Procedures Manual.

4. Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

TERMS AND CONDITIONS

The school network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The school reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the school.

Acceptable network use by school students and staff

1. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
2. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support education and research;
3. The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
4. Staff use of the network for incidental personal use in accordance with all school policies and procedures; or
5. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the school network after checking with the Technology, Media, and Communications Team to confirm that the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all procedures in this document.

Unacceptable network use by school students and staff

1. Personal gain, commercial solicitation and compensation of any kind;
2. Actions that result in liability or cost incurred by the school;
3. Downloading, installing and use of games, audio files, video files, or other applications (including shareware or freeware) without permission or approval from an authorized administrator;
4. Support for or opposition to ballot measures, candidates, and any other political activity;
5. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools, with the exception of educational purposes on a closed network laboratory under the direct supervision of a qualified instructor;
6. Unauthorized access to other school computers, networks and information systems;
7. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
8. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
9. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
10. Attaching unauthorized devices to the school network. Any such device will be confiscated and additional disciplinary action may be taken.

The school will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The school will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the school's computer network or the Internet.

Vandalism

- Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network component. This includes, but is not limited to, the uploading or creation of computer viruses.

Personal Electronic Devices For Staff

In accordance with all school policies and procedures, staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the school.

SOCIAL NETWORKING (STAFF)

Definition: *the use of dedicated websites and applications to interact with other users, or to find people with similar interests to oneself* (Google Dictionary)

TCA realizes that social networking sites and blogs are popular and that they present an opportunity to share with others in a positive way. However, abuses can occur. Therefore, this policy applies to all Internet communications available to the public. All Internet communications during work hours are subject to this policy and the school's Internet and computer-use policy. All employees are expected to reflect a positive Christian testimony and serve as Christian role models, in and out of school. The school's policies against discrimination or other harassment apply to any Internet communications. Therefore, any Internet communications that adversely reflect on the employee's or the school's Christian testimony, that contain confidential student or parent information, that contain confidential school information, that disparage the school or other employees or officers, or that violate the school's anti-discrimination and/or anti-harassment policies may result in requests to remove the communications and employee discipline, including termination. The school shall hold employees personally responsible for all material they post or blog on a website or for content posted by third parties to employee's social-networking or blog Web pages.

Basic Social Networking Rules

The personal use of social networking sites must not interfere with your working time at the school. The Administrator must approve any message that may act as the "voice" or position of the school. Any identification of the author, including usernames, pictures/logos, or "profile" Web pages, should not use any logos or other intellectual property of the school without prior approval of the administration. If employees are not providing an official message from the school, those who comment on any aspect of the school must include a disclaimer in their "profile" or "bio" that the views are their own and not the views of the school. A message should not disclose any confidential information about the school, the students, or the employees of the school. Written messages are, or can become public. Use common sense!

- All social networking activities are subject to all the school policies and procedures.
- Employees should exercise caution in friending or accepting friend requests from current students or parents, alumni or alumni parents. Should you choose to participate in social networking with current students or parents, please be aware that at all times you are a representative of TCA.
- Anything you post including pictures is a reflection of TCA. Remind other members of your network of your position at TCA and that your profile may be accessed by current or former students, and to monitor their posts to your network accordingly. Conversely, be judicious in your postings to all friends' sites, and act immediately to remove any material that may be inappropriate from your site whether posted by you or someone else. Recognize that there is no such thing as complete privacy on a social networking site. Take care in anything you post online. Keep your privacy settings at appropriate levels to protect yourself.

Any postings or communications on social networking sites (Facebook, Twitter, Snapchat, Instagram, and so on) that disrupt the school's learning environment may be subject to investigation and disciplinary action.

PRIVACY

Student Data is Confidential

School staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy

The school provides the network system, e-mail and Internet access as a tool for education and research in support of the school's mission. The school reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

A. The network;
B. User files and disk space utilization;
C. User applications and bandwidth utilization;
D. User document files, folders and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail use.

No student or staff user should have any expectation of privacy when using the school's network or hardware. The school reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all school e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on school servers regularly. Refer to the school retention policy for specific records retention requirements.

Disciplinary Action

All users of the school's electronic resources are required to comply with the school's policy and procedures (and agree to abide by the provisions set forth in the school's user agreement). Violation of any of the conditions of use explained in the Technology Use Agreement, Technology Policies and Procedures (this document), or in the Family Handbook could be a cause for disciplinary action,

including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work

All work completed by employees as part of their employment will be considered property of the school. The school will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the school, the work will be considered the property of the school. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

STUDENT/PARENTS TECHNOLOGY USE AGREEMENT (form)

In consideration for the privilege of using the network and in consideration for having access to the public networks, I hereby release Tacoma Christian Academy, and other intermediary providers, if any, and operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use, or inability to use, TCA's network, including, without limitation, the type of damages identified in the TCA Technology Policies and Procedures.

Further, I agree to abide by the school's Technology Policies and Procedures, which I have reviewed and understand, and I acknowledge that failure to comply with the policy and procedures may result in revocation of network and other technology use privileges.

I acknowledge and agree that Tacoma Christian Academy has the right to review, edit or remove any materials installed, used, stored or distributed on or through the network or school's system including e-mail and other electronic messages and I hereby waive any right of privacy which I may otherwise have into such material. I acknowledge and agree that any copyright I may have in material posted on the Internet through the school's system is waived.

Student's Last/First Name (Print) _____Initials: _____

Parent's Signature _____ Date of Signing ____/____/_____