Electronic Resources Policies and Procedures

Tacoma Christian Academy Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written 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 than face-to-face interactions.

1. Use of the Internet

The question of Internet safety includes issues regarding the use of the Internet, Internet-ready, 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.

Network Use Agreement

Any student or staff member using the Internet from a computer in the school facility must have a valid Individual User Informed Consent Form on file.

Filter

All school-owned computers in all school facilities capable of accessing the Internet must use filtering software to prevent access to obscene, racist, hateful, violent, or otherwise-sinful material.

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 Network Use Agreement, then school staff may instruct the person to cease using that material and/or implement sanctions contained in the Individual User Informed Consent Form.

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.

2. Use of Personal Electronic Devices

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. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day *(See 7. Mobile Device Policy for Students)*

3. Network Use

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 include:

A. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
B. 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;
C. The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
D. Staff use of the network for incidental personal use in accordance with all school policies and procedures; or
E. 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 includes but is not limited to:

A. Personal gain, commercial solicitation and compensation of any kind;

B. Actions that result in liability or cost incurred by the school;
C. 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;
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. 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;
F. Unauthorized access to other school computers, networks and information systems;
G. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
J. 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.

4. Social Networking (STAFF only)

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. School approval is required for employees who use electronic resources of the school to send "tweets" or other public messages on social networking sites. 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.

Participation Rules for School Employees Using School-Sponsored Sites

Social networks allow people to broadcast their thoughts on the Web and collaborate on documents and issues that are interesting and important. It is these elements that create the attraction to this media. As wonderful as these tools are for bringing people together, building relationships, and accumulating knowledge, they can quickly develop into contentious bickering, dialogue, and controversy. Understand that opinions are not necessarily truth or sources of authority. Please exercise "common sense" when using this mode of communication. All school policies must be adhered to in the social network. TCA reserves the right to edit, modify, or delete comments that are inappropriate and that violate the established rules herein. Potential edits include, but are not limited to, removing some or all the information that may threaten the security of individuals or compromise the testimony and integrity of the school. For the benefit of all, the following participation rules apply when posting content to any TCA social network. You agree not to post content characterized by any of the following descriptions: Irrelevant to the subject (moving from business topics to personal), deceitful or deceptive, profane (contains or infers profanity), harmful, abusive, harassing, defamatory, libelous, slanderous, fabricated, misleading, insulting or embarrassing to groups or individuals, threatening in any way, unlawful, pornographic, sensitive and confidential, invasive of another's privacy, infers shouting or uproar (i.e., all CAPS), harmful to minors in any way, discriminatory, misrepresentative of your affiliation with TCA as a person or entity, a chain letter or pyramid scheme, soliciting or promoting a commercial interest, and/or malicious or destructive (i.e., contains software viruses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of any computer software, hardware, or telecommunications equipment). This list is not intended to be complete. TCA reserves the right to add or modify these guidelines at any time.

Guidelines for School Employees Using School-Sponsored Sites

Public social networking is one of the many venues we have established for communication. It is not just about transmitting marketing messaging and fun stuff, but developing relationships with our constituents through authentic conversation that is related to our school mission. Any staff member interested in creating a school social network to communicate with our constituency must complete the Social Network Application. Social network participation is an opportunity for people to share their thoughts and express their opinions about specific subjects and school connections. People designing social network sites under the TCA banner must obtain approval from the school administration. All social network spots must have a clear rationale for existence and adhere to the following guidelines:

All social networks that represent TCA on the Web need to have a domain name that is registered through the school IT department. All domain names, views, comments, and articles posted on those social network sites will be exclusively owned and maintained by TCA. When school staff members are interested in developing a social network site, they must complete an application, which must be authorized through the administration. Upon approval, a domain name will be procured as needed and registered under TCA. All tools and setup procedures must be established within the parameters of the TCA website. The staff members will be given access to Web tools and the social network site within two weeks after approval. All social networks should ultimately be operated and controlled by TCA employees. TCA personnel who manage social network sites must ensure compliance with social network guidelines by approving, modifying, or deleting social network content posted by participants. Rules and guidelines for participation must be clearly stated on the social network sites. All social networks should have a consistent branding that represents the philosophy, ideas, and goals of the school and adheres to the school mission and vision. Management or monitoring of, and response to social network content is the prerogative of the employees who are establishing the social network and must not detract from time required for other work assignments. Approval means that the management of the site is included in the job description of the person or people responsible for monitoring. When starting a social network, care must be taken to avoid disclosing any information that is confidential or proprietary to TCA or to any third party that has disclosed information to us. TCA provides technological equipment for job-related purposes and specifically reserves the right to monitor the employee work performance and use of any

mechanical, electronic, or other work-related device. This includes telephones, voice mail, computer, Internet, Web content, and e-mail. Misuse of TCA equipment may lead to disciplinary action up to and including dismissal. TCA employees who oversee social network sites should demonstrate respect for the school, its employees, its parents, its students, its vendors, and others (including its competitors). People managing social network sites should write and respond while having TCA in mind. They should maintain a consistent witness for Jesus Christ and a humble and courteous attitude in all communications. Free expression, disagreements, and heated debates are common on social networks, but these should never become personal. Avoid posts that may be considered obscene, profane, defamatory, threatening, harassing, abusive, hateful, or embarrassing to another entity. School employees should avoid posts that solicit or promote a business or commercial interest not related to TCA. School employees should avoid posts that contain chain letters or pyramid schemes. School employees should bring controversial content on social network sites to the attention of the school administration, with whom strategies to deal with controversy can be agreed upon. TCA reserves the right to temporarily or permanently suspend inappropriate social network sites or those that violate the established guidelines; threaten the integrity and/or the security of TCA; or violate local, state, or federal law. A social network is media content, and social network postings may generate media coverage, discussions, misunderstandings, differing opinions, differing ideas, and differing theologies. In the event a TCA social network draws media attention for any reason, all such contact must be referred to the school administration so that they can formulate a proper response. All social network postings representing TCA must accurately represent the services, philosophies, and positions of TCA. TCA may approve third-party vendors, affiliates, or partners for social network software and support. To receive approval, these third-party entities must be included on the Social Network Application and receive approval by the Administrator. TCA may not approve third-party vendors, affiliates, or partners for social network software and support if they are deemed incompatible with our Web platform or social network guidelines stated herein. Not everyone who reads TCA social networks will feel comfortable responding to posts if they feel their feedback will become public. In order to maintain an open dialogue that everyone can comfortably engage in, TCA personnel who manage social network sites are asked to welcome "off social network" feedback from colleagues or constituents who would like to respond privately. The acceptance of off-social network comments should be made clear on the social network site. Any photographs or graphics images posted on TCA social networks must have appropriate photo releases and copyright permissions. Any type of intellectual property posted on TCA social network sites must have written permission of the author.
E-mails tied to a social network site should not be personal e-mails. The e-mail addresses should be TCA Google-based accounts and viewed as a school mailbox, and the associated usernames and passwords should be known by more than one person in the school.

5. Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;

B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;

C. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;

B. Any attempts to defeat or bypass the school's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to school browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content);

C. E-mail inconsistent with the educational and research mission of the school will be considered SPAM and blocked from entering school e-mail boxes;

D. The school will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to school devices;

E. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the school; and

F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

G. The school will provide a procedure for students and staff members to anonymously request access to Internet websites blocked by the school's filtering software. The procedure will indicate a timeframe for a designated school official to respond to the request. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request. The school will provide an appeal process for requests that are denied.

Internet Safety 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.

A. Age appropriate materials will be made available for use across grade levels.
B. Training on online safety issues and materials implementation will be made available for administration, staff and families.

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.

6. Network Security and Privacy

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized school purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to school policy;
B. Do not use another user’s account;
C. Do not insert passwords into e-mail or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Do not use the “remember password” feature of Internet browsers; and

G. Lock the screen or log off if leaving the computer.

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 (school's user agreement), Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

7. Mobile Device 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.

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. 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.

Failure to Comply

If a student is caught hiding a cell phone or other mobile device between the hours of 8:10 am and 3:00 pm, the phone 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. The fine for elementary students is $10.00 and increases $5.00 for each subsequent failure to comply. The fine for secondary students is $50.00 and increases $10.00 for each subsequent failure to comply. 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.

Disclaimer

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