Covenant Technology Policy and Agreement

Acceptable Use Policy

Overview

Covenant's intentions for publishing an Acceptable Use Policy are to establish a culture of openness, trust and integrity among students while coming along side students to guide them. Covenant is committed to protecting employees and students from harmful, illegal or damaging actions by individuals, either knowingly or unknowingly.

The Covenant Preparatory School recognizes the value of computers and other electronic resources to improve student learning and enhance the administration and operation of its schools. To this end, the board of trustees encourages the responsible use of computers; computer networks, including the internet; and other electronic resources in support of the mission and goals of Covenant and its schools.

Purpose of AUP

The purpose of this Technology Acceptable Use Policy is to ensure students will benefit from learning opportunities offered by the school's devices and other electronic resources including internet resources in a safe and effective manner. It is the policy of Covenant to maintain an environment that promotes ethical and responsible conduct in all online network activities.

Within this general policy, the Covenant Preparatory School recognizes its ethical obligation to protect the well-being of students in its charge. Although Covenant has taken precautions to restrict access to unappropriated materials, it is impossible to control all materials. Therefore, the responsibility is upon the student or other user not to seek questionable websites or materials.

Acceptable Use

Having access to devices and technology at Covenant is a privilege, not a right. Access to the computing infrastructure is limited to educational purposes. It shall be a violation of this policy for any employee, student, or other individual to engage in activity that does not conform to the established purpose and general rules and policies of the school. Abuse of this privilege will result in disciplinary action.

Only those users who are authorized to speak to or publish media to the public on behalf of the school may represent the school via any electronic communication.

Online Etiquette – Users are expected to express themselves using appropriate language and evaluate the validity of information online.

Unacceptable Use

Online Etiquette – Users should not use abusive, threatening, obscene, harassing, vulgar or suggestive language online or in communications including swearing, slurs or bullying language.

Privacy – Users should not share personal information about themselves, families, or faculty. This includes user account information, passwords, home addresses, phones numbers, birth dates, etc. Users should be aware of privacy settings on any websites they use or subscribe to.

Copyright – Users should comply with copyright laws and fair-use laws while accessing and utilizing online information, software, etc. Copying online information or media without proper documentation or permission will be considered plagiarism.

Images, Videos, Audio Recordings – Users should not record anyone (students, faculty, parents, presenters, school employees) without permission from the specific parties. In addition materials should not be published publicly or privately without consent. This includes on any social media websites. School yearbook staff and students have permission to take photos of school related events for school use only. Users should never record in bathrooms or locker rooms.

No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other materials that is obscene, defamatory, profane, pornographic, harassing, abusive or considered to be harmful to minors.

Users of technological resources may not send electronic communications fraudulently (i.e. by misrepresenting the identity of the sender).

Users may not use technology devices or services (internet/network) of Covenant for any illegal activity or in violation of any school policies. The Covenant Preparatory School assumes no responsibility for illegal activities of students while using technology devices/services.

Instant messaging/texting – Students may not use instant messaging or texting software (apps)/websites.

Peer-to-peer (P2P/file sharing) – students may not engage in peer-to-peer computer use software (app/websites) unless approved by faculty.

Users are not allowed to listen to audio (music), videos online (streaming) for personal use due to the high bandwidth consumption these sources require on the school internet/wifi.

Downloading – Students should not download files/software/apps from the internet without consent from the faculty. Downloading takes considerable bandwidth in most cases and could inhibit network speed of others. Some file types may be blocked from being downloaded altogether.

Users should not tamper with or alter hardware or software on school devices. Including but not limited to hacking activities, “jail breaking” and creation/upload of viruses/malware. Any attempts to circumvent school protective measures incorporated by the school on devices or on the school network will be considered abuse of this policy and disciplinary actions will result. Such things as use of alternative wifi hot spots/internet and anonymizers (proxies) to circumvent firewall restrictions and uninstalling or disabling of monitoring software. Issues with Covenant technology devices, printers or internet connectivity as well as internet content should be reported to IT personnel or email technology helpdesk at helpdesk2@covenantknights.org .

Users should not hinder another’s ability to save or complete his/her work. This includes intentionally powering off someone else’s device or closing device lids.

The heavy usage of school technology increases the challenge of maintaining them in the best possible condition. Students must be good stewards of the devices they use and will be responsible for breakage or tampering of any kind. Breakage as result of student neglect including "playing around" or "rough-housing" will result in the student being financially responsible for repair or replacement of the device.

Covenant has the right to:

- Log network use and to monitor server space utilization by user, and assume no responsibility or liability for files deleted due to violation of server allotments.
- Remove a user account on the network.
- Monitor the use of online activity while on campus or at school sponsored functions, extracurricular activities or athletic events. This may include real-time monitoring of network activity and/or maintaining a log of internet activity for later review. Covenant reserves the right to outsource the monitoring ability to other organizations in the best interest of the safety of their users.
- Terminate any user's access to the internet, at any time for any reason.
- Provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to Covenant owned equipment and specially to exclude those who do not abide by the Covenant Acceptable use policy or other policies governing the use of school facilities, equipment of materials.
- Restrict online destinations through software or other means.

Faculty members who supervise students, control electronic equipment or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of Covenant.

Covenant makes no warranties of any kind, either expresses or implied that the functions or services provided by or through the school's computing infrastructure will be error-free or without defect. Covenant will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service.

Covenant may install internet filtering or monitoring software in an attempt to regulate a user's access to inappropriate and/or harmful context on the internet. All student filtering complies with Children's Internet protection act (CIPA) requirements. Although Covenant has taken precautions to restrict access to questionable materials, it is impossible to control all materials. Therefore, the responsibility is upon the student or other user not to seek questionable websites.

Staff, faculty and upper school students will receive school email addresses. Students and faculty should use their school email accounts for all school communications. School email accounts should be used for school related communications only, no social communications. Students should not use email during class unless specifically instructed by faculty to do so. Covenant faculty and staff may use emails via Student Management System (Renweb) for ease of communication.

Users should save files to their personal folders on the network server or network cloud drive associated with their email or flash drives. Files saved in other locations may be purged without notification. Students should not access devices or folders/files intended for faculty/staff use only.

Students should also shutdown devices upon work completion; they should not lock devices to disallow others from accessing them.

School printers are provided for faculty and students to use to print school related work only.

All guidelines in the technology acceptable use policy apply to school owned devices as well as personal devise brought in for bring your own device (BYOD). Please see BYOD acceptable use policy for specific restrictions on student or faculty personal devices.

Covenant reserves the right to revise this Acceptable Use Policy as it deems necessary and will post the current policy on its website as notice to users of any revisions. Users are responsible for reading the policy regularly.