Westlake Christian Academy
Acceptable Use Policies

STUDENTS

Computer Use Policy

When using the Internet on Westlake computers, students agree to the following:

- You will use the Internet only with a teacher's permission
- You will not visit sites with inappropriate content
- You will not download or install programs or games on Westlake computers
- You will not send or receive e-mail or instant messages without a teacher's permission

Electronic Devices, Social networking and media

Electronic communication/entertainment devices (such as cell phones, mp3 players, game players, etc.) are not to be used unless under the direction of a faculty member. Using any such device in any manner that violates the respect and rights of others is prohibited. Using an electronic device to take photographs, cheat, signal others, or otherwise violate the conduct rules is prohibited. Portable computers (laptops, tablets) may be used for classwork with explicit teacher permission. Appropriate use of approved 1:1 technology (Chromebooks) is acceptable anytime unless redirected by a teacher.

Chromebook use must be in line with the Westlake 1:1 Student and Parent/Guardian Handbook. Westlake utilizes an Internet content filter that is in compliance with the federal Children's Internet Protection Act (CIPA). All Chromebooks, regardless of physical location (in or out of school), have all Internet activity protected and monitored by WCA. If a website is blocked at school, then it will also be blocked when a student is out of school. If an educationally valuable website is blocked, students should contact their teachers to request the site be unblocked. If Westlake discovers that its content filtering service is not functioning, all Chromebooks will be disabled until the filtering service is properly restored.

Parents and teachers must be aware that no content filter is 100% effective and should give appropriate oversight of the students' internet use, whether on the school's computers or the students' managed Chromebooks. Westlake trains students in internet safety to help them understand the risks involved in using such powerful technology.

Students should not attempt to gain unauthorized access to protected school network resources or to circumvent filtering and other security systems. Such activity is a violation of the Child Internet Safety Act and will result in disciplinary action.

Cell phones are to be turned off during school hours. Students may use cell phones before and after school. Cell phone use is not allowed during passing periods, between classes, or at lunchtime. Westlake Christian Academy deems most cell phone usage detrimental to the development of Christian community.

Electronically recording or transmitting video of another person in a restroom or locker room is not acceptable and may be a crime under Illinois law (720 ILCS 5/26-4).

The use of an electronic device in the following manner at any time is unacceptable.

- Capturing, creating, or distributing text, recordings or images of any individual(s) without that individual's consent.
- Capturing, creating, or distributing text, recordings or images of any document(s) which may compromise the integrity of the educational process.
- Capturing, creating, or distributing text, recordings or images of any individual which are disrespectful, embarrassing, or degrading or immoral.
- Capturing, creating, or distributing text, recordings or images which could be reasonably deemed an invasion of privacy, a breach of confidentiality, or a copyright infringement.

Violators of this electronic devices policy will face disciplinary measures and will have their electronic devices (cell phones included) confiscated. Confiscated devices may only be retrieved by a parent. In addition, the student's usage of electronic devices may be restricted.

In today's society, many individuals participate in electronic social networking or media. Students and parents are advised to be wise in text, audio and visual content sent or uploaded onto the Internet. Text, audio, and/or visual content must align with biblical principles and the standards of Westlake Christian Academy. Even off campus, Westlake students and families are responsible for their behavior in these matters.

FACULTY AND STAFF

Faculty and staff are given access to school-owned computer technology as their roles require. Security of such resources is important, not only to safeguard the equipment, but even more importantly to safeguard the integrity and confidentiality of school-owned data, whether located on our internal network or on an external Internet resource. These are guidelines and policies regarding IT at Westlake.

- Each employee is personally responsible for the physical protection of the computer hardware issue to him. To maximize protection of those resources, classroom and office doors must be locked whenever the employee is out of the room, especially at the end of the day.

- Employees who have been issued laptop computers may take them home with the understanding that they are responsible for their repair or replacement if lost, stolen, or damaged.
- Each employee is issued log in credentials to the various soft resources as needed, such as network profiles, WiFi access, copier codes, and Headmaster access. Those credentials should never be shared with anyone else. Students have a generic log in credential which grants access to limited resources on the network. Teachers should rarely allow a student to use a computer which is logged in as a teacher, and then closely supervise.
- Each employee is issued a Westlake email address and is expected to use that account as the primary means of communication with school administration and other personnel concerning matters related to the school. Employees are responsible for information which is disseminated via school-wide and staff-wide email distribution. Teachers should check email and respond daily, but not during teaching time.
- All data stored on the school's network, in Headmaster, and any other cloud-based resource owned by the school is property of Westlake and can be inspected. All email transmission made using the school's email domain may be accessed by the administration if necessary.
- Employees must be very discrete in the use of social media. Comments made on such media which reflect negatively on the employee or the school will result in appropriate corrective measures.
- Employees are responsible to avoid any copyright infringement with regards to computer downloads, uploads, and copier use.
- Employees may personalize the computers issued to them but must ask permission from the IT Director before installing new applications. However, routine maintenance, especially during the summer months, may alter or strip personal settings.
- Westlake uses a filter to protect students and personnel from undesirable Internet content. Employees who find a need to access certain content which has been blocked may ask the IT Director for exemptions. When allowing students to use the internet for research projects, carefully supervise them to make sure they are involved in wholesome and productive activity.
- Westlake computer technology is reserved for educational use and tasks related to the mission of the school. It is not to be used for entertainment. Employees may occasionally use resources for personal use as long as such use does not interfere with employment time or incur costs for the school.
- Employees may access the school's Internet resources via WiFi using their own devises, but they must inform the IT Director of such use and take care never to allow others to see the school's WiFi access key.

- Employees should avoid storing personal data on a school computer or network resource. The school cannot be responsible for safeguarding that data.
- Teachers are encouraged to have a personal cell phone and keep it near them during the day since the school does not have a school-wide telephone system for each classroom. However, personal business should be avoided during teaching time or any time students are within earshot, and ringers must be off during the school day. It is illegal to use a cell phone while driving in the school's parking lot. Teachers must not use their cell phones while supervising students at recess or car dismissal time.