Zephyr ISD

Technology, Network, and Internet User Policy 2023 - 2024

This document contains two pages that must be signed and returned to the school immediately.

Acceptable Use Guidelines for Technology Resources

Zephyr Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the Zephyr schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers and support staff. The use of these technology resources is a privilege, not a right.

With access to computers and people all over the world comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Zephyr ISD firmly believes that the value of information, interaction, and research capabilities available outweighs the possibility that users may obtain material that is not consistent with the educational goals of the district. Zephyr ISD employs several layers of protection and Internet filtering to try to keep out any materials available on the Internet that do not deem applicable to ZISD policies and/or educational practices or that may prove harmful to any of its students or employees. Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Zephyr ISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District Policy.

Definition of District Technology Resources
The District's computer systems and networks are any configuration of hardware and software. The systems and networks include all of the computer hardware, operating system software, application software, stored text, and data files. This includes electronic mail, local databases, externally accessed databases (such as the Internet), CD-ROM, optical media, clip art, digital images, digitized information, communications technologies, and new technologies as they become available. The
District reserves the right to monitor all technology resource activity.

Acceptable Use
The District's technology resources will be used only for learning, teaching and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited. The District will make training available to all users in the proper use of the system and will make copies of acceptable use guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource. Software or external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the Superintendent or designee.

Other issues applicable to acceptable use are:
• Copyright: All users are expected to follow existing copyright laws.
• Student use of the computers and computer network is only allowed on those computers which are designated for student use and which securities have been installed to supervise and filter the student’s use of those computers and Internet.
• The use of instant messaging and social media services such as Facebook will not be allowed to be used within our district system because of the inability to monitor illegal or inappropriate uses of such communication. This is provided for the safety of all users within the ZISD network.

• The use of Internet sites such as YouTube shall be closely monitored by each classroom teacher to ensure that students are accessing information that is intended for educational purposes only.

• Attempting to log on or logging on to a computer or email system by using another's password is prohibited: Assisting others in violating this rule by sharing information or passwords is unacceptable. Improper use of any computer or the network is prohibited. This includes the following:

- Compromising student safety.
- Using social networking websites.
- Using racist, profane, or obscene language or materials.
- Participating in cyber bullying.
- Using the network for financial gain, political or commercial activity.
- Attempting to or harming equipment, materials or data or hacking into District equipment.
- Attempting to or sending anonymous messages of any kind.
- Using the network to access inappropriate material.
- Knowingly placing a computer virus on a computer or the network.
- Using the network to provide addresses or other personal information that others may use inappropriately.
- Accessing of information resources, files and documents of another user without their permission.
- The use of Internet chat rooms is prohibited on all school computers unless approved by the Superintendent &/or his designee. If allowed, these chat sessions would be monitored by a teacher and used for educational purposes only.

System Access

Access to the District's network systems will be governed as follows:

• Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision.

• Students/Teachers with accounts will be required to maintain password confidentiality by not sharing the password with students or others.

• With the approval of the immediate supervisor, district employees will be granted access to the District's system.

• Any system user identified as a security risk or having violated the District's Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also be assigned.

• The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The Superintendent, campus principals, technology director and/or their designees will deem what is inappropriate use and their decision is final. The system administrator may close an account at any time as required or as they deem appropriate without notice.

• The use of personal devices such as PDA's (Palms, Visors, cell phones with web capability, etc) and laptops (either wireless or Ethernet) or any device used to access ZISD networks is prohibited unless special permission is granted from the technology director. Only after the device is deemed to be of minimal or no security risk to the ZISD network will such permission be granted.

• Students who are enrolled in dual-credit courses may use their own personal device for the purposes of completing their dual-credit course. Cell phones are not allowed for this purpose.

Campus Level Coordinator Responsibilities

As the campus level coordinator for the network systems, the principal or designee will:

• Be responsible for disseminating and enforcing the District Acceptable Use Guidelines for the District's system at the campus level.

• Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Individual User Responsibilities
The following standards will apply to all users of the District's computer network systems:
• The individual in whose name a system account is issued will be responsible at all times for its proper use.
• The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district guidelines.
• System users may not use another person's system account without written permission from the campus coordinator or principal, as appropriate.
• System users are asked to purge outdated files on a regular basis.
• System users are responsible for making sure they do not violate any copyright laws.

Vandalism Prohibited
Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any of the agencies or other networks to which the District has access is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district guidelines and, possibly, as criminal activity under applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33. This includes, but is not limited to, the uploading or creating of computer viruses. Vandalism as defined above will result in the cancellation of system use privileges, possible prosecution, and will require restitution for costs associated with system restoration, hardware, or software costs. The willful introduction of computer “viruses” or other disruptive/destructive programs into the District’s network or into external networks is prohibited.

Forgery Prohibited
Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

Information Content/Third Party Supplied Information
System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems outside the District's networks that may contain inaccurate and/or objectionable material.
A student bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

Network Etiquette
System users are expected to observe the following network etiquette (also known as netiquette):
• Use appropriate language: swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language is prohibited.
• Pretending to be someone else when sending/receiving messages are prohibited.
• Transmitting obscene messages or pictures is prohibited.
• Revealing such personal information as addresses or phone numbers of users or others is prohibited.
• Using the network in such a way that would disrupt the use of the network by other users is prohibited.
• Be polite.

Off Campus Device Policy
• All policies in this document apply to ZISD owned technology being used off-campus as well as on-campus.
• The use of checkout out devices at home is encouraged.
• Device care at home is as important as in school, please refer to the vandalism section of this document.

Termination/Revocation of System User Account
The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.
Termination of an employee's account or of a student's access will be effective on the date the principal or campus coordinator receives notice of user withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Consequences of Improper Use
Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

Disclaimer
The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor supplied hardware and software. Therefore, the District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's computer systems and networks. Network storage areas may be treated like school lockers. Network administrators and/or their designees may review files and communications to maintain system integrity and insure that users are using the system properly. Users should not expect that files stored on District servers would always be private.

Internet/Technology Safety Training
The student body of Zephyr ISD will receive Internet and technology safety training during the beginning of each school year. Emphasis will be given in regards to: safety on the Internet, appropriate behavior while online, on social networking websites, and in chat rooms. Cyber bullying will be addressed with special emphasis as well as any other issues that should be addressed in regards to the school district Technology Acceptable Use Policy. The training will be given by the District Technology Director or technology teacher at an age appropriate level for the students. Students will sign a form after the training each year to document that they have received the training.

Zephyr ISD employs a filtering program to minimize access to inappropriate web sites for its students. The filtering software is a commercially produced filter product that attempts to block possibly objectionable sites. No filter is perfect. Zephyr ISD will not accept responsibility of student's disregard of the District's policies and guidelines as they relate to Internet access.

STUDENT AGREEMENT *(This must be renewed each school year)*

I understand and will abide by the above **Zephyr ISD User Policy** for network and Internet use. I also agree to report any misuse of the information system to a staff member. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal actions may be taken.

Student Name: _____

Student Signature: _____ Date: _____

PARENT OR GUARDIAN PERMISSION

As the parent or guardian of this student, I have read the Zephyr ISD User Policy for network and Internet use. I understand that this access is designed for educational purposes. I also recognize that it is impossible to restrict access to all controversial materials and will not hold Zephyr ISD responsible for materials acquired on the network, but I do recognize that the school will use all resources available to make my child's Internet experience as safe as possible.
Furthermore, I accept full responsibility for supervision if and when my child's use is not in the school setting. I understand this access enables my son/daughter powerful opportunities and responsibilities to become a learner of the 21st century. **I hereby give permission to issue a technology use account for my child and certify that the information contained at the bottom of this form is correct.**

Student Name: _____

Parent or Guardian Signature: _____ Date: _____

PARENT OR GUARDIAN TO <u>DENY</u> PERMISSION

I do not wish my child to have individual access to the Internet.
(Leave blank if this does not apply.)

Student Name: _____

Parent or Guardian Signature: _____ Date: _____

USE OF PHOTOGRAPH/DIGITAL VIDEO PERMISSION
(This must be renewed each school year)

Zephyr Independent School District would like to include your child on our school website or in public presentations during the school year. This may occur in the form of a photograph or digital video. As always, Zephyr ISD strives to uphold the safety and protection of your child and will exercise caution in any digital media that appears on our website or internal network. If it deems necessary to associate a student's name with a picture, it will only appear in the form of their first name and last initial. (Ex: Jane D.) We request your permission to use his/her photograph and first name with last initial.

(Please check one of the following)

☐ Yes, I do agree to allow my child to appear on the school website or other school presentations along with his/her first name and last initial by either photograph or video. I understand that Zephyr Independent School District will exercise caution in how this media will be used.

☐ I agree to allow my child's picture to appear on the school website or other school presentations by photograph or digital video, but I **do not** want his/her name to appear. I understand that Zephyr Independent School District will exercise caution in how this media will be used.

☐ No, I do not wish my child to appear on any school media by either picture, video, or name.

Student's Name _____

Parent/Guardian's Signature_____

Date _____