STUDENT INTERNET ACCEPTABLE USE POLICY

Introduction

The Internet is a place for the exchange of information and ideas on a wide range of subjects. With access to computers and people all over the world also comes the availability of materials that may not be considered to be of educational value in the context of the school setting. The Zionsville Community Schools' (ZCS) network is connected to the Internet. While ZCS implements Internet filtering on all ZCS sites, it is impossible to control all materials on a global network. As such, students may encounter materials that are obscene, abusive, or otherwise offensive. ZCS firmly believes that information and the interaction available utilizing the network outweighs the possibility that students may access materials that are not consistent with the educational goals of ZCS. Internet access is seen as a supplement to traditional sources, both print and non-print, not as a replacement for them. The purpose of this policy is to identify standards that will assist in ensuring students benefit from their use of the ZCS network and the Internet.

Use of the ZCS Network

The use of the ZCS network is a privilege, not a right. Students who fail to comply with this policy or violate ZCS' disciplinary policies while using the ZCS network may lose the privilege to access the ZCS network. Students may also lose the privilege to use computer equipment provided by ZCS or to bring their own computerized devices to school. Students may also be subject to other disciplinary action as appropriate based upon the nature and severity of the violation. During student registration, parents will complete and sign a Student Internet Access / Computer Use Agreement with ZCS.

Services

Internet provides access to:

A. Electronic mail communications with people all over the world.

B. Information and news from government, other public agencies, as well as the opportunity to correspond with scientists, authors, and politicians from around the world.

C. Discussion forums on a variety of topics.

D. Library catalogs and other materials from the Library of Congress, the Smithsonian, the Indiana State Library, and many universities.

Acceptable Uses

Acceptable use of Internet resources is based on its original purpose, which is to provide a backbone network to support research and education in and among academic institutions in the United States by providing access to unique resources and the opportunity for collaborative work. The operation of this worldwide computer network relies upon the proper conduct of its users. As a result, individuals must adhere to appropriate use guidelines.

ZCS does not assume responsibility for individuals using the network through its facilities, but does acknowledge the responsibility to the Internet community to enforce accepted standards of network protocol and the obligation to recommend the termination of a user's network capabilities if misuse of the Internet resources is discovered.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media.

Use of the Internet by ZCS students must be in support of education and research and must be consistent with the educational objectives of the corporation. During classroom activities, it is the responsibility of the classroom teacher to supervise student Internet use in a manner that is consistent with the educational objectives of ZCS and this policy.

Unacceptable Uses

Use of the ZCS network for any of the following purposes is prohibited:

- To knowingly access, upload, download, or distribute or attempt to knowingly access, upload, download or distribute pornographic, obscene, or sexually explicit materials.
- To transmit or attempt to transmit obscene, abusive, or sexually explicit language, images, or materials.
- To annoy, harass, intimidate, or threaten, or attempt to annoy, harass, intimidate, or threaten any person or organization.
- To vandalize, damage, or disable, or attempt to vandalize, damage, or disable the property of another person or organization.
- To endanger or attempt to endanger the integrity of a computer on the ZCS network or the data stored on the network, including the introduction of computer viruses or worms.
- To circumvent or attempt to circumvent ZCS's Internet security measures and/or filters.

- To log on or to attempt to log on to the network using another person or group's name and password or to otherwise misuse a name or password.
- To falsely represent or attempt to falsely represent oneself in any Internet communication.
- To access or attempt to access another person's materials, information, or files without the implied or direct permission of that person.
- To transmit or attempt to transmit, without authorization, information that is false or defamatory or violates the privacy of another person.
- To interfere with or attempt to interfere with the lawful activities of any person, business, or organization in any manner.
- To violate or attempt to violate copyright, or otherwise use another person's intellectual property without his/her prior approval or proper citations.
- To transmit or attempt to transmit, without authorization, copyrighted materials or materials protected by trade secret.
- To transmit or attempt to transmit unsolicited emails (e.g., chain letter emails, spamming emails) or emails to any of ZCS's distribution lists without permission of a school official.
- To download or attempt to download games, entertainment software, or copyrighted material without permission of a school official.
- To utilize peer-to-peer file-sharing applications or attempt to utilize peer-to-peer file-sharing applications without permission of a school official.
- To install or modify or attempt to install or modify any software on any ZCS computer.
- To engage in commercial activity, product advertisement, or political lobbying.
- To violate or attempt to violate any local, state or federal statute, or any rule, regulation, or policy of ZCS.

This is not an exhaustive list. Other similar behaviors are prohibited and may subject a student to the denial of privileges, disciplinary action, and/or referral to appropriate law enforcement agencies.

Data Privacy and Protections

ZCS strives to be transparent with all processes related to the collection, retention, security, and termination of data. Zionsville Community Schools' policies and procedures for securing all Personally Identified Information(PII) and student data protection are located at http://www.zcs.k12.in.us/apps/pages/data_privacy.

In accordance with its obligations under the Children's Internet Protection Act, ZCS implements measures to block or filter, to the extent practicable, access to material that is obscene, pornographic and/or harmful to minors. Because of these monitoring obligations, students have no expectation of privacy in any aspect of their use of the ZCS network or any computer equipment, software, access accounts, or other types of materials or facilities owned, controlled, or provided by ZCS. Use of the ZCS network constitutes consent to be monitored.
ZCS reserves the right to view, copy, intercept, or block the transmission of any type of material or communication which does not conform to this policy, and may use any such material or communication in the investigation of any violation of this policy or in any disciplinary actions or proceedings against any student which might result from the student's violation of this policy. ZCS also reserves the right to make referral of certain types of violations to appropriate law enforcement agencies.

Student Responsibilities

In accordance with its obligations under the Children's Internet Protection Act, ZCS has undertaken efforts to educate students about appropriate online behavior, including cyberbullying awareness and response and interactions with individuals on social networking websites and in chat rooms.
Students using the network and communicating with others on the Internet should exercise caution and remember the following:

- People in chat rooms on instant messaging may not be who they appear to be.
- Personal information, such as home telephone numbers, names, addresses, and photographs of students, should never be disclosed in a public forum (e.g., a chat room or on a profile).
- Students should not reveal their names or personal information to or establish relationships with strangers met through the Internet, unless a parent or school official has coordinated the communication.
- Internet security is tenuous at best. Students should refrain from sending or receiving any communications or material over the network that they would not want to be made public.
- Do not respond to unsolicited emails, advertisements, or other requests for your personal information.
- Protect your password by making it long and strong (combining upper and lowercase letters with numbers and symbols).
- If a student is uncomfortable or feels harassed, intimidated, or threatened by information that he or she receives over the Internet, he or she should tell a teacher, principal, or other school official immediately. Likewise, if a student is asked by another Internet user to stop emailing or contacting them, the student must stop all contact immediately.
- If a student receives inappropriate materials or stumbles onto inappropriate materials on the Internet while doing legitimate research, the student is expected to notify the teacher, principal, or another school official.

Network etiquette expects that the student abide by the following guidelines. These guidelines include, but are not limited to:

- Students are expected to be courteous and respectful. The use of vulgar, obscene, lewd, and otherwise inappropriate language is prohibited. Students shall not engage in cyberbullying.
- While the Internet itself has virtually boundless resources, the availability of local communication and storage resources is limited. Since list servers and mail servers can generate a significant amount of data to be stored, students are expected to "clean up" their files or mailboxes at appropriate times so as to not create a storage problem on the host server.
- All communications and information obtained via the network or the Internet should be assumed to be intellectual property subject to federal copyright law.
- Any attempt to compromise network security is prohibited. Any student identifying a possible breach in security must notify a system administrator or the corporation's Chief Technology Officer.

Information and Service Disclaimers

ZCS makes no warranties of any kind, whether expressed or implied, about the information gained through the Internet, including its quality or accuracy. Use of information obtained through the Internet is at the student's own risk and ZCS cannot be held responsible for any material a student mistakenly or intentionally accesses or transmits via the ZCS network.

ZCS makes no warranties about the quality of the services provided and is not responsible for any claims, losses (including, but not limited to, the loss of data), damages, costs, or other obligations arising from a student's use of the ZCS network or any computer equipment or software owned, controlled, or provided by ZCS.

It is the policy of ZCS that the cost of any materials to a student utilizing the Internet is the responsibility of the student, or in the case of a student under the age of 18, the person who authorizes a network account. This authorization extends to any financial obligation that may be incurred when utilizing the network. Under no circumstances will ZCS be liable for any unauthorized purchases or other financial obligations resulting from ZCS-provided access to the Internet. The signatures on the Internet Access / Computer Use Agreement are legally binding and indicate that the party (parties) who signed has (have) read the terms and conditions carefully, understand the significance of the policy, and agree to abide by the policy in all its terms and conditions.

USE OF WIRELESS COMMUNICATION DEVICES

The Board of School Trustees permits students to bring personal laptops or other computing devices to school for academic purposes. Use of these devices is at the discretion of the teacher and administration. The purpose of this policy is to ensure that students and their parents/guardians understand the obligations and limitations associated with the use of personal laptops or other devices. These guidelines are a supplement to the school's Internet Acceptable Use Policy, which applies to the use of any computing device in school, including personal laptops and other devices.

Guidelines for Use

- Use of a personal laptop or other computing device is at the discretion of the administration and teacher. Students must obtain permission before using such a device in class.
- Use of a personal laptop or other device must support instructional activities.
- Students must agree to disable audio/video functions and to put away a personal laptop or other device, if asked.
- Students may only use personal laptops or other devices in accordance with Zionsville Community Schools' Internet Acceptable Use Policy.
- A violation of any of these guidelines may result in the revocation of privileges regarding the use of a personal laptop or computing device and appropriate disciplinary and/or legal action.

A "wireless communication device" is a device that emits an audible signal, vibrates, displays a message, or otherwise summons or delivers a communication to the possessor. The following devices are examples of WCDs: cellular and wireless telephones, pagers/beepers, personal digital assistants (PDAs), Blackberrys/Smartphones, Wi-Fi-enabled or broadband access devices, two-way radios or video broadcasting devices, laptops, and other devices that allow a person to record and/or transmit, on either a real time or delayed basis, sound, video or still images, text, or other information. Students may not use WCDs on school property or at a school-sponsored activity to access and/or view Internet websites that are disruptive to the school activity. Students may use WCDs while riding to and from school on a school bus at the discretion of the bus driver. Distracting behavior that creates an unsafe environment will not be tolerated.

Using a WCD to take or transmit audio and/or pictures/video of an individual without his/her consent maybe considered an invasion of privacy. Students who use a WCD to violate the privacy rights of another person may have their WCD confiscated and held.

WCDs, including but not limited to those with cameras, may not be possessed, activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower facilities, restrooms, classrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The building principal has authority to make determinations as to other specific locations and situations where possession of a WCD is absolutely prohibited.

No expectation of confidentiality will exist in the use of WCDs on school premises/property.

Students are prohibited from using a WCD in any way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated. See Policy 5517.01 – Bullying and Other Forms of Aggressive Behavior.

Students are also prohibited from using a WCD to capture and/or transmit test information or any other information in a manner constituting fraud, theft, cheating, or academic dishonesty. Likewise, students are prohibited from using their WCDs to knowingly receive such information.

Possession of a WCD by a student is a privilege that may be forfeited by any student who fails to abide by the terms of this policy, or otherwise engages in misuse of this privilege.

Violations of this policy may result in disciplinary action and/or confiscation of the WCD. The building principal may also refer the matter to law enforcement if the violation involves an illegal activity (e.g. child pornography). Discipline will be imposed on an escalating scale ranging from a warning to an expulsion based on the number of previous violations and/or the nature of or circumstances surrounding a particular violation. Any search of a WCD will be conducted in accordance with Policy 5771 – Search and Seizure. If multiple offenses occur, a student may lose his/her privilege to bring a WCD to school for a designated length of time or on a permanent basis.

Restrictions and Disclaimers

- The Corporation accepts no responsibility or financial liability for personal laptops or other computing devices that are brought to school by students.
- Laptops or other devices that are lost, stolen, or damaged are the responsibility of the student and his/her parents/guardians, regardless of how the loss, theft, or damage occurs.
- Students are advised to take steps to guard against damage, loss, or theft.
- ZCS' technology department will not provide technical support for any personal laptop or other computing device.

Technical Requirements for Access

- Personal laptops or other computing devices must conform with ZCS technical requirements, which are accessible through the ZCS website and which may be amended from time to time.