Acceptable Use for Technology Resources

The Coppell 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 within Coppell ISD 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 many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Coppell ISD firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, email, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District.

Proper behavior, as it relates to the use of technology resources, is no different than proper behavior in all other aspects of Coppell ISD activities. All users are expected to use all technology resources in a responsible, ethical, and polite manner. This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with District policy.

Acceptable Use

The District's Acceptable Use for Technology Resources Policy is to prevent unauthorized access and other unlawful or improper activities by users online, prevent unauthorized disclosure or access to sensitive or confidential information, ensure appropriate use of its technology resources, and to comply with the Child's Internet Protection Act. As used in this policy, "user" includes anyone using the District's technology resources, including computers, Internet, e-mail, chat rooms, wireless network, and other forms of direct electronic communications or equipment provided by the District. Only current students, employees, officers, volunteers and authorized visitors of the District are permitted to use the District's technology resources and network.

Students who are under 18 must have their parent(s) or guardian(s) authorize student use of the District's technology resources and acknowledge compliance with this policy. Students who are 18 or older, as well as employees and other users, must acknowledge their compliance with this policy, either electronically online or by signing and returning a copy of the acknowledgement form provided below. The absence of a signed acknowledgment does not excuse compliance with this policy. All users must follow this policy and report any misuses of the District's technology resources to a teacher, supervisor, administrator or appropriate District personnel. By using the District's technology resources, users are held to have agreed to comply with this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult District personnel in advance of any questionable use.

Violation of computer use policies, rules, or agreements may result in the user's access being suspended or having access completely revoked for a time period determined by district administration, as well as additional disciplinary or corrective action.

The use of any technology resource (including, but not limited to, desktop computers, personal/CISD devices, network-delivered services, the Internet, audio-visual equipment, digital content and social media) must support the educational goals of Coppell Independent School District. Use must be authorized by a CISD staff member and must lie within the bounds of CISD curriculum and educational purpose.

CISD computers, personal/CISD devices, the Internet, and all other technology resources should not be used for personal, commercial or financial gain or to otherwise conduct business that is unauthorized.

When placing, removing, or restricting access to specific databases, the Internet and/or any other technology resource, school officials shall apply the same criteria for educational suitability used to evaluate all other educational resources. Please refer to EFA Local (Instructional Resources: Instructional Materials Selection and Adoption) located in the Coppell ISD School Board Policy Manual

(http://www.tasb.org/policy/pol/private/057922/pol.cfm).

Individual(s) involved in any of the following will be subject to disciplinary or corrective action in accordance with applicable District policy, handbooks, rules and regulations:

a. Possessing, accessing, transmitting, copying, or creating material that violates the Student Code of Conduct, District policy, student or employee handbooks, or District rules and regulations, including but not limited to content that is inappropriate, illegal, copyrighted, pornographic or obscene, stolen, threatening, discriminatory, harassing, or offensive.
b. Attempts to bypass or disable the District's Internet filter, security systems or software.
c. Attempts to access, alter, interfere with, damage, or change network configuration, security, passwords, or individual accounts of another without written permission from the CISD Technology Department.
d. Any unauthorized attempts to circumvent passwords or obtain access to passwords or other security-related information.
e. Disclosing any other user's password to others or allowing another individual to use another's system account.
f. Attempts to upload, create, or transmit computer viruses.
g. Attempts to access or install unlicensed, inappropriate, or unapproved software or technology.
h. Attempts to alter, destroy, hack, or disable District computer equipment, personal/CISD devices, District data, the data of others, or other networks connected to the District's system, including while off school property.
i. Plagiarism or use of District technology resources to engage in academic dishonesty.
j. Use of District technology resources to create, send or post electronic messages or communications that are abusive, profane, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
k. Unauthorized use of any District technology resource or personal/CISD device for non-educational purposes or outside the bounds of CISD curriculum.
l. Use of e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct that violates the Student Code of Conduct, or threaten school safety.
m. Use of District technology resources, including e-mail, the Internet or social media resources to threaten, harass, bully, retaliate, discriminate against, or otherwise engage in illegal or prohibited conduct against other students, employees, or volunteers.
n. Use of personal e-mail, the Internet, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment
o. Violating or infringing upon the intellectual property, copyrighted or trademarked rights of another.
p. Possessing, accessing or transmitting any material which is considered inappropriate or is in violation of any federal or state law is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secrets.

These are examples of inappropriate conduct that would violate this policy. The District reserves the right to take immediate disciplinary or corrective action against a user that engages in conduct that: (i) creates security or safety issues for the District, students, employees, schools, networks, or technology resources, or (ii) is determined to be inappropriate or inconsistent with District policy or law.

Individual User Responsibilities

All users are expected to abide by the generally accepted rules of network etiquette (also known as netiquette). These rules include, but are not restricted to the following:

1. BE POLITE AND USE APPROPRIATE LANGUAGE: Remember that you are a representative of your school and District on a non-private system. You may be alone using a technology resource or personal/CISD device, but what you say and do on your computer can be viewed globally. You should not submit, publish or display any defamatory,

inaccurate, racially offensive, discriminatory, abusive, obscene, profane, sexually oriented, harassing or threatening materials or messages either public or private.

2. PRIVACY: Do not reveal any personal information about yourself or other persons (including, but not limited to, home address, personal phone numbers, photographs, or last name).

   Users should have no expectation of privacy regarding their use of District property and technology resources. In general, communications or transmissions made through technology resources should never be considered private or confidential. The District reserves the right to monitor the use of its network and all technology resources as it deems necessary to ensure the safety and integrity of its network, diagnose problems, investigate reports of illegal or impermissible activity and ensure user compliance with state and federal laws and the District's policies. In addition, users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its technology resources, including e-mail communications.

3. ELECTRONIC MAIL:
   a. All users of any electronic mail either provided by the District or transmitted through the District's technology resources are required to comply with this Acceptable Use Policy.
   b. System users are asked to purge email or outdated files on a regular basis. Employees and volunteers should ensure that any official school records that are maintained in an electronic medium that are subject to state or federal retention requirements are either retained in hard copy or archived prior to being deleted or purged.
   c. Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.
   d. Be brief and professional: Few people will bother to read a long message or one that is not narrowly tailored to the underlying purpose of the communication. Electronic communications by District employees, volunteers and staff should be consistent with the District's professional standards of conduct.
   e. Include your signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.
   f. Send only to individuals and/or groups you know.

4. DISRUPTIONS: Do not use the network in any way that would disrupt use of the network by others.

5. OWNERSHIP: Any data or communication placed on District equipment will become the property of CISD. Intellectual property created solely for the purpose of satisfying a course requirement and/or contributing to their student learning is owned by the creator.

6. VANDALISM: Any attempt to alter or destroy data of another user will be subject to disciplinary or corrective action in accordance with District policy.

7. ACCOUNTABILITY: Users are responsible for the proper use of their system accounts, passwords and District-issued technology resources. Users must control unauthorized use of their accounts, passwords and District-issued technology resources. Users should not provide their password to any person, unless authorized or directed by the District. If you permit someone else access to your account, password, or District-issued technology resources, you may be held responsible for any improper, illegal or destructive activity done by that person. Do not give others access to District technology resources unless they are authorized and authenticated to do so. Users may not extend access to District technology

resources to others without permission from the District.

If you believe that your account, password or District-issued technology resource may have been stolen, hacked, or compromised, you must immediately report it to the District's Technology Department.

Internet Safety

The Coppell Independent School District makes the Internet accessible in accordance with our mission to provide information resources and services to ensure that all users have free and open access to ideas and information. In this role, the District provides access to information resources available on the Internet. The District has no control over the information obtained through the Internet and cannot be held responsible for its content or accuracy. It may contain materials which some find offensive or inappropriate. All staff, students and other users access the Internet at their own discretion.

In accordance with the federal Children's Internet Protection Act (CIPA), (Pub. L. 106-554), all desktop computers, laptops and personal/CISD wireless devices, that utilize the CISD network, will be filtered by a centralized filtering appliance. This filtering appliance is set to screen out sites which may reasonably be construed as obscene, as that term is defined in section 1460 of title 18, United States Code; or child pornography, as that term is defined in section 2256 of title 18, United States Code; or harmful to minors as defined in section 1703, Pub. L. 106-544. The District has the ability to monitor the online activities of students and staff through direct observation and/or technological means to ensure that students and staff are following the guidelines and policies set forth by the District.

District Board Policy also prohibits harassment, bullying, retaliation, discrimination, and other conduct that creates a hostile working or educational environment for an individual. This prohibition extends to the use of the District's technology resources. If you ever feel that you are being harassed, bullied, retaliated or discriminated against, or otherwise being subjected to illegal or inappropriate conduct through the District's technology resources, you should immediately report it to the District.

As with any other technology resource, restriction of a child's use of the Internet is ultimately the responsibility of the parent/legal guardian, within the confines of the law.

The District assumes no responsibility for damages, direct, or indirect, for the use of the Internet. This includes, but is not limited to, damage to District or personally owned equipment caused by virus-laden material downloaded from any Internet site. Users are encouraged to purchase and use a virus detection program on their personal devices.

Users should be aware that the Internet is not a secure medium. It is possible for third parties to obtain information regarding an individual user's search activities. Users should be very cautious about providing personal information over the Internet.

Definitions

Social Media: the interactive use of online resources including, but not limited to, Facebook, YouTube, Twitter, MySpace, Ning, Google Apps, Skype, chat rooms, wikis, and blogs.

Children's Internet Protection Act (CIPA): The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

Personal Devices: the use of any technology related device that is not owned by Coppell ISD.

Digital Content: products available in digital form. It typically refers to music, information and images that are available for download or distribution on electronic media.

Hacking: to re-configure or re-program a system to function in ways not facilitated by the owner, administrator, or designer.

Copyrighted: The legal right granted to an author, composer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.

Computer Virus: a computer program that can copy itself and infect a computer. It is also being used as a catch-all phrase to include all types of malware, adware, and spyware programs that do not have the reproductive ability. Malware includes computer viruses, worms, trojans, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with computer worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan is a program that appears harmless but hides malicious functions. Worms and Trojans, like viruses, may harm a computer system's data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious and go unnoticed.

Technology Resources: Any and all mass storage media, online display devices, computers, computer printouts, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, receiving, storing, managing or transmitting data including but not limited to mainframes, servers, personal computers, notebook computers, laptops, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, telecommunication devices, network environments, telephones, fax machines and printers. Technology resources also includes the procedures, equipment, facilities, software and data that is designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display and transmit information.

Parental Restriction on use of Technology Resources

Parents who have objections to the Internet or other network-delivered services may assume responsibility for imposing restrictions only on their child(ren). Any parent wishing to restrict his/her child's access to such services must provide the school with this restriction in writing. For details, see the CISD board policy governing the selection and adoption of instructional materials.

Acknowledgement of Policy

Users must either acknowledge this policy electronically (online student registration system or Student Code of Conduct for students, Employee Handbook for staff or submit their acknowledgment and signature of this form to the appropriate campus and/or department as a prerequisite to their use of the District's technology resources.

ACKNOWLEDGEMENT: I have read, understand, and agree to abide by the provisions of the District's Acceptable Use for Technology Resources policy.

_____
USER'S NAME

_____
USER SIGNATURE

_____
PARENT/GUARDIAN SIGNATURE (If User is Student under 18)

_____
DATE