Computer & Network Acceptable Use Policy

Southwest Area Technology Team Collaborative Draft Policy

Please Note: When a student signs the Acceptable Use Policy individually or in a handbook, it is also referring to this and other Board Approved and published District Policies. The Federal Law Appendix is located at the end of this document.

Please return this agreement, signed by student and parent, to your homeroom teacher.

<District Name> provides a wide array of technology resources for student use. This agreement, along with any student handbooks in each school, outlines appropriate use and prohibited activities when using technology resources. Every student is expected to follow all guidelines stated below, as well as those given orally by the faculty & staff, and to demonstrate good citizenship and ethical behavior at all times.

<u>In accepting this agreement, students acknowledge the following rules and conditions:</u>

As a <District Name> student, I understand that my school network and email accounts are owned by the District and are not private. <District Name> has the right to access my information at any time.

GOVERNMENT LAWS:

I will use computers in conformity with laws of the United States and the State of Utah. Violations include, but are not limited to, the following:

1. Criminal Acts – These include, but are not limited to, “hacking” or attempting to access computer systems without authorization, harassing email, cyberstalking, child pornography, vandalism, and/or unauthorized tampering with computer systems. (A list of Federal statutes from the United States Department of Justice is below as Appendix A).
2. Libel Laws - Publicly defaming people through the published material on the Internet, email, etc…
3. Copyright Violations - Copying, selling or distributing copyrighted material without the express written permission of the author or publisher (users should assume that all materials available on the Internet are protected by copyright), engaging in plagiarism (using other's words or ideas as your own).

NETIQUETTE and RESPONSIBLE USE:

1. I understand that passwords are private. I will not allow others to use my account name and password, or try to use that of others.
2. I will be polite and use appropriate language in my email messages, online postings, and other digital communications with others. I will not use profanity, vulgarities or any other inappropriate language as determined by school administrators.
3. I will use email and other means of communications (e.g. blogs, wikis, chat, instant-messaging, discussion boards, etc.) responsibly. I will not use computers, cell phones, personal digital devices or the Internet to send or post hate or harassing mail, make discriminatory or derogatory remarks about others, or engage in bullying, harassment, or other antisocial behaviors.
4. I understand that I am an Ambassador for the school in all my online activities. I understand that what I do on social networking websites such as MySpace and Facebook should not reflect negatively on my fellow students, teachers, or on the District. I understand that I will be held responsible for how I represent my school and myself on the Internet.
5. I understand that using school computers or networks to masquerade, spoof, or pretend to be someone else is forbidden and potentially illegal. This includes, but is not limited to, sending out e-mail, creating accounts, or posting messages or other online content (e.g. text, images, audio or video) in someone else's name as a joke.
6. I will use District computer resources responsibly. I will not retrieve, save, or display hate-based, offensive or sexually explicit material using any of the Districts computer resources. I am responsible for not pursuing material that could be considered offensive. I understand that I am to notify a school employee immediately if by accident I encounter materials that violate appropriate use.
7. I will use District technology resources productively and responsibly for school-related purposes. I will not use any technology resource in such a way that would disrupt the activities of other users.
8. I will not attempt to bypass security settings or Internet filters, or interfere with the operation of the network by installing illegal software, shareware, or freeware on school computers.
9. I understand that vandalism is prohibited. This includes but is not limited to modifying or destroying equipment, programs, files, or settings on any computer or other technology resource.
10. I will respect the intellectual property of other users and information providers. I will obey copyright guidelines. I will not plagiarize or use other’s work without proper citation and permission.
11. I will not use or access files, software, or other resources owned by others without the owner’s permission. I will use only those District network directories that are designated for my use or for the purpose designated by my teacher.

12. I will follow all directives set forth by the District and/or my teachers when publishing schoolwork online (e.g. to a website, blog, wiki, discussion board, podcasting or video server).
13. I understand the Internet is a source for information that is both true and false; and that the school is not responsible for inaccurate information obtained from the Internet.
14. I understand that the District administrators will deem what conduct is inappropriate use if such conduct is not specified in this agreement.
15. I agree to abide by all Internet safety directives that are provided by the school and to complete all assignments related to Internet safety.

CONSEQUENCES FOR VIOLATION OF THIS AGREEMENT:

I understand and will abide by the above Acceptable Use Agreement. Should I commit a violation, I understand that consequences of my actions could include suspension of computer privileges, school disciplinary action, referral to law enforcement, or other appropriate and reasonable consequences.

Student Signature: _____

Date _____

Parent or Guardian:

As the parent or guardian of this student, I have read the Acceptable Conduct and Use Agreement. I understand that computer access is provided for educational purposes in keeping with the academic goals of <District Name>, and that student use for any other purpose is inappropriate. I recognize it is impossible for <District Name> to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the District network if students receive reasonable and responsible supervision and Internet filtering is in place. I understand that at times Internet filtering is not perfect, and may not be effective 100% of the time. I understand that children's computer activities at home should be supervised as they can affect the academic environment at school.

I hereby give permission for my child to use computer resources at <District Name>.

Parent or Guardian's Name (please print)
_____

Parent or Guardian's Signature _____

Date _____

Appendix A –
Unlawful Online Conduct and Applicable Federal Laws

The chart below details the type of unlawful online conduct, potentially applicable federal laws, and the section of the Department of Justice with subject-matter expertise. If the subject matter expert is not a section of the Department, but rather another agency, the entry will have an asterisk following its initials. In many cases, prosecutors may also consider whether the conduct at issue is a violation of 18 U.S.C. § 2 (aiding and abetting) or 18 U.S.C. § 371 (conspiracy).

Unlawful Conduct	***Applicable Federal Law***	***DOJ Section***
Denial of Service Attacks	18 U.S.C. § 1030 (a)(5)(A) (transmission of program, information, code, or command, resulting in damage)	CCIPS
	18 U.S.C. § 1362 (interfering with government communication systems)	CCIPS
Use of Misleading Domain Name	18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material)	CEOS
Password Fraud	18 U.S.C. § 1030 (a)(6) (trafficking in computer passwords)	CCIPS
	18 U.S.C. § 1029 (access device fraud)	Fraud/ CCIPS
	18 U.S.C. § 1343 (wire fraud)	Fraud
Obscenity	47 U.S.C. § 223 (a)(1)(A) (using telecommunications device to make, create, or solicit, and transmit any obscene comment, request, suggestion, proposal, image, or other communication)	CEOS
	18 U.S.C. § 1465 (using interactive computer service for purpose of sale or distribution of obscene material)	CEOS
Piracy and Intellectual Property Theft	17 U.S.C. §§ 1201-1205 (Digital Millennium Copyright Act)	CCIPS
	17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement)	CCIPS
	18 U.S.C. § 2319A (trafficking in recordings of live musical performances)	CCIPS

Electronic Threats	18 U.S.C. § 875 (transmitting communications containing threats of kidnap or bodily injury) (Hobbs Act)	CTS
	18 U.S.C. § 1951 (interfering with commerce by robbery, extortion, threats or violence) (Hobbs Act)	DSS
	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to threaten person who receives communication)	CCIPS
Electronic Harassment	47 U.S.C. § 223 (a)(1)(C) (anonymously using telecommunications device to harass person who receives communication)	CCIPS
	47 U.S.C. § 223 (a)(1)(E) (repeatedly initiates communication with a telecommunication device solely to harass person who receives communication)	CCIPS

Unlawful Conduct	***Applicable Federal Law***	***DOJ Section***
Interception of Electronic Communications	18 U.S.C. § 2511 (intercepting electronic communications)	CCIPS
	18 U.S.C. § 2701 (accessing stored communications)	CCIPS
	18 U.S.C. § 1030 (a)(2) (accessing a computer and obtaining information)	CCIPS
Cyberstalking	18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family) See also Electronic Harassment	DSS
Hate Crimes	Look to civil rights laws and penalty enhancements	Civil Rights
Libel/Slander	Look to civil laws	
Posting Personal Information on a Website (e.g.,	This is not a violation of law, but could be a violoation of District Web Publishing policies.	

phone numbers, addresses)		
Invasion of Privacy	*See Interception of Electronic Communications*	
Disclosure of Private Information	18 U.S.C. § 2511 (1)(c) (disclosing intercepted communications)	CCIPS
Spam	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS
Spoofing Email Address	18 U.S.C. § 1037 (CAN-SPAM Act)	CCIPS