COMPUTER NETWORK AND INTERNET ACCESS AND USE

AUTHORIZATION FOR NETWORK/INTERNET ACCESS

A. Definition. The Network/Internet refers to the global network of computers created by the interfacing of smaller contributing networks. Its services are intended to support curriculum, instruction, open educational inquiry and research, and legitimate business interests of Sweetwater County School District Number One, State of Wyoming ("the District"). In this document, "Network/Interface Access" refers to all information accessed through the use of the District's equipment and resources for connection to and use of the Network/Internet online services, including, but not limited to, electronic mail ("e-mail"), messaging systems, collaboration systems, social networking, bulletin boards, and network conferencing systems.

B. Philosophy of Network/Internet Use. The goal of the District is to include appropriate Network/Internet access in the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication including access to online libraries and databases for educational or research use. All use of District Internet access and District networks will conform to the requirements of all District Policies. Access to the Network/Internet must be for the purpose of education, research or legitimate business interests of the District, and must be consistent with the educational objectives of the District. The Network/Internet access is provided knowing that some information provided by institutions and individuals available online may include material that is not for educational or research use in the context of a public school. Some information may be inaccurate, abusive, profane, sexually oriented or otherwise in violation of applicable law. The District supports responsible use of the Network/Internet and does not condone or permit the use of inappropriate material.

C. Authorized Users. Administrators, teachers, other employees of the District, and students may be authorized to use the Network/Internet, which includes all information accessed by Network/Internet sites, e-mail, online services, and bulletin board systems. Access to the Network/Internet is granted as a privilege, not a right. Individual users of the Network/Internet consent and agree to use the Network/Internet in an appropriate and responsible manner and by their use, behavior or communication shall not violate any Policy of the District or applicable law. Access to the Wyoming Equality Network and the Sweetwater #1 Network is coordinated through various government agencies, regional networks, and private entities. Authorized users consent and agree to follow applicable guidelines of each respective agency, network or entity providing Network/Internet access.

D. Students. Each student is deemed to have consent and authorization from his or her parent(s) or legal guardian(s) for Network/Internet access prior to using the District's Network/Internet connection. Any student of legal age or his or her parent(s) or legal guardian(s) may withdraw consent and authorization for Network/Internet access for the current school year by completing the STUDENT'S WITHDRAWAL OF NETWORK/INTERNET ACCESS form and submitting it to the school where the student is enrolled.

STUDENT USE OF THE NETWORK/INTERNET

The following safety and acceptable-use provisions with respect to Network/Internet use should be discussed by parent(s) or legal guardian(s) with their students, and students agree and consent to abide by such provisions:

1. The Network/Internet may only be used for appropriate educational purposes.
2. The Network/Internet may be used to collaborate with others for educational or research purposes.
3. Students should not divulge personal information such as social security numbers, personal addresses, personal telephone numbers, parents' work addresses or telephone numbers without parental permission.
4. Students should tell their parents, school administrators or teachers immediately if they come across any information that makes them feel uncomfortable or that they find threatening.
5. Students should never agree to get together or meet someone that they "meet" online without first checking with their parent(s) or legal guardian(s).
6. Students should never send anyone their picture or any other item without first checking with their parent(s) or legal guardian(s).
7. Students should tell their parent(s) or legal guardian(s) immediately if they receive any such message.

PRIVACY

Users will have no expectation of privacy regarding files or messages stored on District-based computers. Electronic messages and files stored on school-based computers or stored outside of school using the District's Network/Internet account are deemed to be property of the District. Consequently, users should not have any expectation of privacy with respect to their files or messages. The System Administrator, Building Principal and his/her designees may review files and messages at any time to maintain system integrity and insure that the users are acting responsibly. The District utilizes technologies to remotely monitor and manage users. The District reserves the right to capture any and all packets traversing the Sweetwater #1 Network.

In compliance with the Children's Internet Protection Act (CIPA) Sweetwater County School District Number One, State of Wyoming uses specific technology protective measures to block or filter access to inappropriate matter or visual depictions prohibited by law.

UNACCEPTABLE USE OF DISTRICT COMPUTER NETWORK AND INTERNET
Uses which are unacceptable under the Policy because they cause substantial disruption of the proper and orderly operation and discipline of the school, violate the rights of others, constitute socially inappropriate use, are inappropriate due to the maturity level of the students, or are primarily intended as an immediate solicitation of funds, include, but are not limited to, the following:

1. Using the Network/Internet for any illegal activity, including violation of copyright, intellectual property rights, or other contracts or transmitting any material in violation of any United States or State law or regulation, or District Policy;
2. Using, sending or receiving copyrighted material in violation of the copyright;
3. Unauthorized downloading of software**,** scripts, music or any other document or file, regardless of whether it is copyrighted;
4. Using the Network/Internet for private, financial or commercial gain;
5. Gaining unauthorized access to resources or entities, including, but not limited to, other student files,

teacher files, confidential information and student record data;

6. Invading the privacy of individuals, including revealing the personal addresses or telephone numbers of students, teachers or administrators;
7. Circumventing security, filtering and/or authentication measures, including using another user's account or password;
8. Posting materials authored or created by another without his/her consent;
9. Posting anonymous messages and/or falsifying one's identity to others while using the system;
10. Using the Network/Internet for commercial purposes or private advertising, solicitations, promotions, destructive programs (viruses or self-replicating code) or any other unauthorized use;
11. Accessing, searching, submitting, posting, publishing, transmitting, receiving or displaying pornographic, indecent, obscene, lewd or vulgar content, or foul, profane or abusive language;
12. Submitting, posting, publishing or displaying libelous material;
13. Using the Network/Internet while access privileges are denied, suspended, or revoked;
14. Using the Network/Internet in any way that would disrupt its use by other users, including but not limited to "chain letters," uploading or creating computer viruses or self-replicating code, and any other attempt to harm or destroy data of another user, the Sweetwater #1 Network any other network or system connected to the Network/Internet;
15. Using the Network/Internet for the purpose of harassing, torturing, tormenting or abusing other users or other individuals;
16. Installation of unauthorized software on District computers and networks;
17. Use of the system to alter documents or records, create a forged instrument or otherwise commit forgery;
18. Accessing the Network with unauthorized devices connected via Ethernet, USB, FireWire, Blue Tooth, Thunderbolt, IEEE 802.11x(a, b, g or n), Infrared or any other wireless signals;
19. Using Bootable devices (e.g. USB devices, CD's, DVD's Firewire devices, External harddrives) to gain access or alter the function of a computer or a network;
20. Accessing or using personal and 3rd party email accounts (the District will provide all students in grades 5 through 12 with an email account to be used in the educational setting);
21. Participating in online chat rooms or using instant messaging for non-educational purposes;
22. Using District computers and networks for non-educational purposes (e.g. games, gambling, role playing and multi-user scenarios and games).

USE OF DISTRICT COMPUTING AND TECHNOLOGY EQUIPMENT

Students must use district computing and technology equipment in a responsible way. Students damaging District computers, mobile devices or technology equipment will be responsible to pay for repair(s) or replacement(s). Legal parent/guardian of students participating in a one-to-one laptop or mobile device program(s) will be required to sign a contract detailing the guidelines for laptop use as well as care of the laptop or device.

USE OF PERSONAL COMPUTING & NETWORK ACCESSIBLE EQUIPMENT

Personal Computers, Mobile Devices or other network accessible devices (owned by the student) may be used on school premises only after receiving approval by the building administrator and the classroom teacher. The District encourages the use of Personal Devices to assist with a student's education. Personal devices may NOT be connected to the district network until they have been inspected and verified by the Information Technology Department. Some devices will be required to have Anti-Virus software, Anti-Spyware software and Firewall capabilities. The District reserves the right to determine the best method for connecting, controlling and servicing these devices. Devices not conforming to this policy will be denied access.

USE OF COLLABORATION TECHNOLOGIES FOR EDUCATIONAL PURPOSES

The District will utilize controlled and public collaboration technologies. These technologies may include but are not limited to (Podcasting, Blogging, Wikis, Video Conferencing, Instant Messaging, RSS Feeds, Personal Learning Networks, Social Networking, etc.). Students will be instructed on the proper use of these technologies. Students using these technologies in an un-safe, inappropriate or offensive way will forfeit their right to participate and use these collaboration technologies.

DISTRICT ASSIGNED SERVER ACCOUNTS AND EMAIL ACCOUNTS

The District may elect to assign students email accounts and server accounts for storage and management of classroom work. Email accounts are for education purposes only. These email accounts will be subject to filtering and random monitoring. Student server accounts will also be subject to random monitoring. Any student violating this policy or abusing the use of these accounts will have their account(s) suspended. Students should never share server or email passwords. Student email accounts and server accounts will be archived per the District's Electronic Document Storage & Retention policy.

SECURITY

Security is a high priority. If the user can identify a security problem on the Network/Internet, the user must notify the supervising teacher, Building Principal, or System Administrator. The user may not demonstrate the problem to other users and must keep their account and password confidential. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. Any user identified as a security risk may be denied access to the Network and/or Internet.

NO WARRANTIES

A. The District makes no warranties of any kind, whether expressed or implied, for the service of providing Network/Internet to its users, and bears no responsibility for the accuracy or quality of information or services or the loss of data. The District will not be responsible for any damages any user suffers, including loss of data resulting from delays, non-deliveries, missed- deliveries, or service interruptions caused by the District, 3rd parties or users' errors, omissions, or negligence. A user's ability to connect to other computer systems through the Network/Internet or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems. Use of any information obtained via the Network/Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the Network/Internet.

B. The District assumes no responsibility for any authorized charges or fees, including telephone charges, long distance charges, per minute surcharges, data plan charges and/or equipment or line costs.

INDEMNIFICATION

The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees incurred by the District relating to, or arising out of, any violation of this Policy and any unauthorized charges or fees, including, but not limited to, telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

COOPERATION WITH INVESTIGATIONS

The District reserves the right to cooperate fully in any investigation requested by parties alleging to be impacted by the conduct or use of computer equipment on the Network by any user and further reserves the right to turn over any evidence of illegal or improper activity to the appropriate authorities.

ENFORCEMENT

The failure of any user to abide by this Policy will result in the denial, revocation, or suspension of the Network/Internet privilege, disciplinary action, and/or appropriate legal action. Denial, revocation or suspension of the Network/Internet privilege and/or disciplinary action will be determined by the Building Principal or his/her designees.

LEGAL REFS.: Children's Internet Protection Act, Public Law 106-554, 47 U.S.C. § 254
Adopted: 1/22/96
Revised: 6/24/02 5/23/05 6/27/05 3/27/08 6/22/08 10/13/08 6/11/12 2/9/15

School District #1, Sweetwater County, Wyoming