SWEETWATER COUNTY SCHOOL DISTRICT #1

Agenda Item 13-c

Recommendation for the approval of Policy GBCE (Computer Network and Internet Access and Use)

COMPUTER NETWORK AND INTERNET ACCESS AND USE
STAFF

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 board(s), and network conferencing systems.

~~B.~~ *Covered by Acceptable Use Policy* ~~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 education 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~~ Unified 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. In addition, volunteers, continuing education students, educational professionals not employed by the District, or designated community members may be granted permission to use the Network/Internet for educational purposes as a privilege, not a right. Authorization for such use may only be granted by a member of the District's Administration, the Building Principal, or the ~~Director of Technology~~ Chief Information Officer.

D. Staff Use. Each certified staff member and those classified staff members desiring computer access must sign the District's "Staff Authorization for Network/Internet Access" prior to using the District's Network/ Internet connection.

STAFF USE OF THE NETWORK/INTERNET

The following safety and acceptable-use provisions with respect to Network/Internet use apply to all staff use of the District's computers and Network/Internet access, and staff agrees and consents to abide by such provisions:

1. The Network/Internet may be used for appropriate educational purposes or for legitimate business purposes of the District.
2. The Network/Internet may be used for e-mail to collaborate with others for education, research or legitimate business purposes of the District.
3. Staff should not give out personal information or confidential information of students, including grade or other non-directory information except to the person in interest. *See* Policy File JO.
4. The Network/Internet may be used for personal email providing the email content does not violate any District policies and the email cannot contain attachments or act in a malicious manner. Sending or forwarding jokes, "chain letters," gambling, solicitations, for-sale items, pictures or music files is strictly prohibited. Personal emails may not exceed 5000 characters or 15K in size.
5. The network/Internet may be used for personal purposes during non-school hours providing the activity does not violate any District policies and does not interfere with on-going or special District business. Users understand that any personal research interfering with District business must be halted when asked and the user may be temporarily disconnected from the Network/Internet so the District may complete the required business. Any costs or charges incurred as a result of personal research are the sole responsibility of the User.
6. The Network/Internet may be used for SEA general information and communication (meeting notices, issues resolution, FYI items). SEA communications must adhere to all District policies for email content.

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.

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~~

Covered by Acceptable Use Policy

~~Uses which are unacceptable under the Policy 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 via solicitation copyrighted material in violation of the copyright;~~
3. ~~Unauthorized downloading of software, music or any other document or file, regardless of whether or not 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, classified and certified employees, administrators or parental information;~~
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, soliciting, submitting, posting, publishing, transmitting, receiving via solicitation or displaying pornographic, indecent, lewd, obscene, 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 "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 or 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 the computer Network;~~
17. ~~Use of the system to alter documents or records, create a forged instrument or otherwise commit forgery;~~
18. ~~Accessing or using personal and 3rd party email accounts (the District will provide employees with an email account to be used in conjunction with their job function and for educational purposes). Staff members are permitted to utilize college and continuing education-based email accounts for the purposes of professional development, recertification and continuing their education;~~
19. ~~Participating in online chat rooms and using instant messaging for non-educational purposes;~~
20. ~~Using Bootable devices (e.g. USB devices, CDs, DVDs, Firewire devices, External hard drives) to gain access or alter the function of a computer or a network;~~
21. ~~Using district computers and networks for non-educational purposes (e.g. games, gambling, role playing and multi-user scenarios and games).~~

USE OF PERSONAL DEVICES

Staff members are permitted to use Personal Computers, Mobile Devices and other Network Accessible Devices on the Sweetwater #1 Network. However, prior to their use, the Staff member must obtain permission from their immediate supervisor and the ~~Director of Technology~~ Chief Information Officer. 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.

~~SECURITY~~ *Covered by Security Incident Procedures Policy*

~~Security is a high priority. If the user can identify a security problem on the Network/Internet, the user must notify the Building Principal or Director of Technology Chief Information Officer. The user may not demonstrate the problem to other users and must keep the user's 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 user's 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 up to and including termination of employment, 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, Administrator or his/her designees.

HARDWARE, SOFTWARE AND NETWORKING COMPONENTS

A. Property of the District. Hardware, software and networking components purchased by the District

are the sole property of the District. All District computers shall have Network Management Software, chosen by the District, installed and enabled at all times. The Network Management Software includes, but is not limited to, network use authorization and security, remote desktop management, remote monitoring and packet capturing. All District computers shall have a computer and network access software lock enabled at all times. Users may not bypass or alter this feature. The District may assign or reassign hardware, software and networking components to any individual or building at any time without prior notification. The District may also upgrade, modify, or disable hardware, software and networking components at any time without prior notification.

B. Authorization for Removal. All hardware, software and networking components assigned to a particular building, classroom or office must remain in the assigned location, including associated components such as keyboard, mouse and cable. Hardware, software and networking components may not be removed from assigned District premises without prior written authorization from the Building Principal or the ~~Director of Technology~~ Chief Information Officer. All signed authorizations for removal of hardware, software and networking components will be filed with the Technology Center.

C. ~~SOFTWARE LICENSING~~ All software to be installed on Sweetwater County School District #1 computers must be approved by the ~~Director of Technology~~ Chief Information Officer prior to installation. All software must have appropriate licenses prior to installation

LEGAL REFS.: Children's Internet Protection Act, Public Law 106-554, 47 U.S.C. § 254

Adopted: 1/22/96
Revised: 3/10/03 1/22/07 03/27/08 5/11/09 10/8/12

School District #1, Sweetwater County, Wyoming