Terms and Conditions

Governing Use of

Sweetwater County School District #2

Technology Resources

October, 2008

Terms and Conditions Governing Use of District Technology Resources

Summary

The computer system that you are accessing is the property of Sweetwater County School District No. 2 and is to be used only for legitimate educational and business purposes. There is no expectation of privacy for users of the system, including e-mail, files stored on district systems, and web browsing. The use of the system is monitored, and misuse will result in disciplinary action including termination and criminal prosecution for violations.

Purpose

This document clarifies the applicability of law and District policies to technology usage. It also defines new guidelines and procedures where existing policies do not specifically address issues particular to the use of technology.

The purpose of this document is to;

- Inform the District community about the applicability of policies and laws for technology usage and electronic data,
- Inform the users of technology equipment and services about technology department procedures,
- Inform users of electronic data services about how concepts of privacy and security apply to electronic data,
- Help ensure Technology equipment and electronic data services are used in compliance with policies and laws,
- Minimize disruptions to District technology services,
- Provide answers to procedural questions,
- Minimize potential problems and liabilities.

Scope

Authorization to use the District's technology resources is granted to students, faculty, school board members and staff for legitimate District purposes to assist them in their jobs. Authorization can be extended to Substitutes and non-district employees if the building administrator and central administration approve such a request to benefit the district.

Legal Ramifications

Both law and District policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic data services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Policies are also in place which governs the use of the physical equipment as well, including checkout policies, disposal, and determination of vandalism. Under certain circumstances, the law contains provisions for felony offenses.

Use of District Technology Resources must comply with all Federal, State and Local Laws and all District Policies. Unauthorized or improper use may be a violation of the Federal Electronic Communication Privacy Act (See Appendix) and/or Wyoming State Statutes 6-3-501 through 6-3-505, and/or District Policies. Other laws and policies may apply. Violations will result in disciplinary action that may include loss of access, fines of $250,000 and/or imprisonment.

Allowable Uses

District Related Work

The District's technology resources are supported by public funds and are to be used primarily for District related work. Proper use includes using the resources for homework, class projects, sanctioned research

projects, business operations of the District, classroom enhancement, or use directed by a District administrator, faculty, school board members.

District electronic mail services are to be limited primarily to District faculty, school board members and staff for educational purposes and professional communication only.

Software must be used in compliance with the terms of the applicable license agreements.

Personal Use

District electronic services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not: (i) directly or indirectly interfere with the District operation of technology resources or electronic services; (ii) burden the District with noticeable incremental cost; or (iii) interfere with the user's, or any other user's employment or other obligations to the District; **Excessive personal use is grounds for disciplinary action, and an employee's personal use of the Network is tracked and monitored.**

Prohibited Activities

Inappropriate or Unlawful Material

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, threatening or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communications or displayed on or stored on Sweetwater County School District No. 2 computers, web pages or file servers. Users encountering or receiving this kind of material should immediately report the incident to their supervisor or the Assistant Superintendent.

Financial Gain/Purchases

District technologies may not be used for personal financial gain or to purchase items for personal use. Examples include, posting or purchasing items on online services such as eBay, purchasing items from online market places such as QVC, Sears, JC Penny, etc. If the purchase is for educational purposes it must follow district purchasing guidelines.

Interference and/or Waste of Computer Resources

District services must not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, unwarranted or unsolicited interference with others' use of electronic systems, or an unfair monopoly of resources to the exclusion of others. Such acts include, but are not limited to:

- sending or forwarding email chain letters,
- "spamming," that is, send unsolicited e-mail to persons with whom you do not have a prior relationship,
- sending "letter-bombs," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email,
- using district resources to promote or advance ones political ideas or candidates,
- downloading entertainment software,
- playing games,
- engaging in online chat groups,
- using social networking sites (examples Facebook, MySpace, etc),
- use of instant messaging software,
- downloading or using non-approved software,
- printing multiple copies of documents,

- streaming audio and/or video from a Web site or server.
- saving excessive amounts of personal entertainment files (music, video, photos). The district will not maintain data storage for these purposes and will require users to remove files of this nature from District network storage.

Snooping

Information stored on the District's technology resources is considered an electronic extension of an individual's personal work area. It cannot be inspected, copied, or otherwise tampered with unless the owner gives permission, except during administration of the facilities by Technology Staff, as demanded by due process of law, or as determined to be in the best interests of the District.

Misrepresentation

Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the District unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the District. An appropriate disclaimer is: "These statements are my own, not those of Sweetwater County School District #2."

False Identity

Users shall not employ a false identity, or use another person's account.

Altering Attribution Information

Users must not alter the "From" line or other attribution-of-origin, information in e-mail, messages or postings. Users should identify themselves honestly and accurately when posting to newsgroups, sending e-mail or otherwise communicating online.

Destructive Software

District Technology Resources may not be used for creating, disseminating, using or storing destructive programs (i.e., viruses or self-replicating code), intrusion utilities (i.e. hacking tools), or any other destructive code, except by District Technology security personnel in the performance of their job functions. Such use requires the written permission of the Technology Supervisor. Any software installed or used on District Technology Resources must be approved by the Technology Supervisor prior to installation.

Virus Contamination

Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the District's network. All material received on any external media and all material downloaded from the Internet or from computers or networks that do not belong to the District must be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops might contain viruses. All disks, thumb drives, CD's, e-mails, or other electronic media transferred from these computers to the District network must be scanned for viruses. Users may not attempt to disable or otherwise circumvent any virus scanning or spyware checking utilities.

If you suspect that a virus has been introduced into the district's network, notify the District Call Center immediately.

Connectivity to District Resources

The district provides network connectivity using copper, fiber, or wireless means for the purpose of connecting District computing resources to file servers, internet, or network attached resources. Users may not connect any personal devices to the network as we cannot install the monitoring software, or remote agents on any non-district computer. Personal equipment may not have the latest virus definitions, updates, or security protocols in place and may introduce viruses into the network, or interfere with bandwidth requirements during critical times such as testing windows. Exceptions will be granted for

trainers, visiting dignitaries, state officials, and auditors. The Technology Department will create special quarantine networks for them to attach to for a specified period of time.

Software Piracy and Copyright Infringement

Making unauthorized copies of copyrighted computer software is an infringement of federal copyright laws and is always in violation of a license agreement. Such violations can result in large costs to the District and to the individual(s) involved. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy.

Users may not do any of the following:

- Illegally copy, post, or download material protected under copyright law or make that material available to others for copying,
- Copy software for use on their home computers, unless it is explicitly allowed by license agreement and approved by the Technology Department,
- Install software on any of the District's computers,
- Modify, revise, transform, recast, or adapt any software,

Web Site Creation and Maintenance

The District may provide, buildings, and teachers the ability to create and maintain a web site on the District web servers. This privilege requires that users make every effort to ensure that all information is current, accurate, and protects the privacy of students and staff.

Users may not do any of the following:

- Illegally post, material protected under copyright law or make that material available to others for copying,
- Post links to sites that are banned by the District,
- Use this web site as a personal page for online dating, applying for jobs with other entities, or promoting political parties, candidates or ideals,
- Post student pictures, or work, (individual, group, or otherwise), without written consent from the student's guardian and approval from the building administrator, using technology form TWR-01-A.
- Posting student names or any portion of their name is prohibited.
- Post information that is defamatory, slander, or libelous.

Sites will be inspected on a regular basis and any site violating any regulation of this section or any section of the Terms and Conditions will be immediately removed and disciplinary action will take place.

Phone Use

Phones are provided by the District for the purpose of communication with patrons, administrators, and staff members. Web services may be added to the phone to enhance the functionality of the phone, access to those services still fall under the guidelines set forth in this document for internet use. In addition users are to limit personal calls into the phone system, as well as limit long distance calls that are not related to work. Voicemail like, e-mail, has no expectation of privacy, and can be used during an investigation, or during system maintenance.

Cautions

The nature of electronic mail and the public character of the District's business make electronic mail less private than user may anticipate. Users should be aware of the following:

- Users should never consider electronic communications to be either private or secure,
- Electronic mail (e-mail) intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others,
- A reply to an email message posted on an electronic bulletin board or "list server" intended only for the originator of the message may be distributed to all subscribers to the list server,
- Even after a user deletes an email record from a computer or account, it may persist on backup facilities and be subject to disclosure under other legal provisions.
- Computer viruses can spread through the electronic messaging system. Do not open any enclosures when you are unsure of the contents,
- The district is unable to give an employee an ability to "retract" an email message once it is sent,
- System administration personnel with high security clearances have access to private electronic communications,
- Users of District email services should be aware that Wyoming Statutes and other similar laws jeopardize the ability of the District to guarantee complete protection of personal email resident on district facilities,
- There is no guarantee that email received was in fact sent by the purported sender. It is a violation of District Policy for sender to disguise their identity,
- Email that is forwarded may also be modified. In case of doubt, receivers of email messages should check with the sender to validate authorship and authenticity,
- The Technology Department will make every effort to protect users from receiving electronic mail they may find offensive in accordance to the District's harassment policy. However, due to the nature of SPAM and phishing scams, messages of this type may find its way into the system. If a user receives SPAM or phishing scams they must send the message to emailabuse@sw2.k12.wy.us for processing. It is the responsibility of the user to report the receipt of offensive, harassing material to the Assistant Superintendent or supervisor.

Disclaimer of liability for use of Internet

- Sweetwater School District #2 is not responsible for material viewed or downloaded by users from the Internet. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. Users accessing the Internet do so at their own risk.

Blocking of Inappropriate Content

The District has the right (but not a duty) to use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by District networks. In the event you encounter inappropriate or sexually explicit material, immediately disconnect from the site, regardless of whether

the site was subject to District blocking software, and report the issue to your Supervisor or the Technology Supervisor. The use of proxy sites and services by users to bypass the filters that are in place will result in immediate suspension of internet access pending a full investigation.

Personal Data

Personal data should not reside on local or file server hard drives. No attempt will be made to ensure the preservation or integrity of personal data. If users are found to have excessive amounts of personal data they will be asked to remove said data from the file servers by a specified date and the issue will be reported to their supervisor. If users have not removed their personal data after said date, the data will be removed by the technology staff.

Special Provisions

Waiver of privacy rights

Users expressly waive any right of privacy in anything they create, store, send, or receive while utilizing District Technology facilities. Users consent to allowing personnel of the District to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that the District may use human or automated means to monitor use of its Technology Resources

Confidentiality

The confidentiality of electronic data cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

Legal Requirements on Privacy of and Access to Information, prohibits District employees and others from "seeking out, using, or disclosing" without authorization "personal or confidential" information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records.

Student and employee records contained in the electronic Student Information System are highly confidential, and access is to be used only for appropriate District business. Unauthorized access and/or distribution of confidential student information and/or misuse of access are subject to disciplinary and legal action.

Users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of District email services, and on these and other occasions may inadvertently see the contents of email messages.

Responsibility for Passwords

Users are responsible for safeguarding their passwords, keys and access codes for access to the District's technology facilities. Individual passwords must not be printed, stored online, written down, or given to others. Users are responsible for all transactions made using their passwords. No user may access the District's facilities with another user’s password or account. Passwords must meet the minimum password requirements adopted by the school district, and will comply with settings that may prevent the use of certain passwords or the reuse of passwords after a specified period of time. Passwords for the Student Information Systems, Finance Systems may have different password requirements, but users must not write down, share or distribute these usernames or passwords as well. The Technology Staff will never ask a user for their Windows, Student Information System, or Finance System passwords. Other methods of authentication may be implemented either in place or in conjunction with passwords, including, biometrics, smartcards, and PIN numbers.

Passwords do not Imply Privacy

Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The District's technology staff has global passwords that permit access to all material stored on District technology facilities - regardless of whether that material has been encoded with a particular User's password.

Accessing Another User's Files

Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another user does not imply permission to read, alter, or copy that file. Users may not use district technology facilities to "snoop" or pry into the affairs of other users by unnecessarily reviewing their files and e-mail.

Accessing other Computers and Networks

A User's ability to connect to other computer systems through the network, VPN, or other remote services 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.

Facilities Security

Each user is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of the District's Technology Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the District's network without authorization and to prevent introduction and spread of viruses.

District Equipment

The Technology provided to the users is paid for by public funds, and is intended for the use of performing ones job duties, and enhancing the education of the students. Users are not allowed to take any district technology resource outside of the building without prior approval of the Technology Staff, and signing checkout form TCF-01. The use of District Technology outside of District grounds still binds the user to all agreements, policies, and regulations adopted by Sweetwater County School District Number 2. The user also agrees that this technology is being used for legitimate District business. Loss or damage of such equipment will require that the user pays for the replacement or repair costs incurred by the district.

Software Installations

The Technology Department will authorize all software installations and document all installations in the District's software inventory.

Personal software with a legitimate educational purpose may be use with District owned technology facilities under the following circumstances:

- Use is approved by Principal or Supervisor, and
- Testing is completed by technology department and compatibility with district facilities is confirmed, and
- Install media, copy of license agreement, proof of purchase and a letter temporarily transferring license to the District is on file with the technology department, and
- Technology staff does the installation.

Monitoring and Inspections

The District has the right, but not the duty, to monitor any and all aspects of its technology system, including, but not limited to, monitoring Internet sites visited by users, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.

The District shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such email (i) when required by and consistent with law; (ii) when there is substantiated reason to believe that violations of law or of District policies have taken place; (iii) when there are compelling circumstances; or (iv) under time-dependent, critical operational circumstances.

District employees are expected to comply with District requests for copies of electronic records in their possession that pertain to the administrative business of the District, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by the District. Failure to comply with such requests is a violation of this policy

Technology staff members may read electronic data only if it is necessary to recover, repair or maintain a technology resource, server or service. In the event such non-consensual access occurs, all information must be kept confidential and the owner must be promptly notified. Reading another person's electronic data without consent for any reasons other than those stated is a violation of District policy.

Violations

Violations will be taken very seriously and may result in disciplinary action, included possible termination, and civil and criminal liability.

Employees who become aware of any misuse of District technology resources or violation of this policy should report the incident to the Technology Supervisor, immediate supervisor or the fraud and ethics hotline immediately.

State and/or Federal Statutes

Various statutes cover computer crime and include definitions and remedies for (1) crimes against intellectual property, (2) crimes against computer equipment and supplies, (3) crimes regarding interruption or impairment of governmental operations or public services, and (4) crimes against other computer users. Violation of these laws can be considered either misdemeanors or felonies, depending upon the circumstances. These laws provide for steep fines and/or imprisonment.

Service Restrictions

Violations of District policies governing the use of District technology resources and services may result in restriction of access to District information technology resources, and other disciplinary actions, including suspension and termination.

Access to District electronic services, when provided, is a privilege that may be wholly or partially restricted by the District without prior notice and without the consent of the user when required by and consistent with law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established district-wide procedures or, in the absence of such procedures, to the approval of the appropriate administrator.

Investigating Suspected Improper Use

The Technology Department may investigate any complaint or indication of misuse or theft of the facilities it operates. During an investigation, only administrators authorized Technology personnel and, as appropriate, law enforcement personnel, may review data, programs, computer activity traces, or backup information, which are pertinent to the investigation. During an investigation of improper use, any person implicated may be denied access to the facilities.

Remedies

Any hearing, appeal or disciplinary action, which results from misuse or theft of technology facilities, will be conducted according to District Policies. In addition to any administrative actions provided by District policies, any suspected violation of a state or federal law will be referred to the appropriate law enforcement agencies for independent investigation.

Duties and Responsibilities

District

The District may be required by contracts, or by discovery demands in litigation, or by lawful demands from law enforcement authorities, to search and turn over District records, including email sent or received by District employees.

District employees are warned that the electronic messages they send and store are District property and may one day be required to be disclosed to other parties.

End-Users

It is every user's duty to use the District's technology resources responsibly, professionally, ethically, lawfully and in accordance with this policy.

Technology Department

The District Technology Staff has an obligation to perform periodic software audits and to correct any violation discovered.

Notification and Acknowledgement

It is mandatory for all users to read and accept, in writing, the Technology Resources Terms and Conditions before they can log on or use any district technology resource. A copy of this Acknowledgement will be placed in the employees personnel file.

Amendments and Revisions

The policies and/or guidelines may be amended or revised from time to time as the need arises. All users will be sent amendments to the policies in electronic form. A printed copy will be made available to each building to post. Users may request printed copies from the Technology Department. Amendments to policies will posted 15 days prior to taking effect. Any person logging onto the computer 15 days after such notification will signal their acceptance of the amendment, and bind one to that policy. If a revision to the terms and conditions takes place which warrants one to sign the agreement again, users will have 60 days to sign and return said document.

Acknowledgement of Terms and Conditions Governing Use of Sweetwater County School District No. 2 Technology Resources

I have read and agree to comply with the policies, rules, and conditions governing use of Sweetwater County School District No. 2 Technology Resources. I understand that a violation of this agreement will be taken seriously and will result in disciplinary action, including possible legal action and termination. I have read and agree to these terms.

Date:_____

Signature:_____

Printed Name:_____

Terms and Conditions Revision 10/2008