

Twin Falls School District #411

Computer and Network Use Policy

201 Main Avenue West
Twin Falls, Idaho 83301

Telephone: 208-733-6900
Fax: 208-733-6987



Technology users' responsibilities go beyond general care of computers and the computer room. Twin Falls School District's policy addresses the acceptable use of technology hardware, software, networks, and the Internet.

Unless otherwise specified, the following regulations will apply equally to students, employees, volunteers, and contractors employed by the Twin Falls School District. Employees, volunteers, and contractors may have additional obligations owing to the nature of their positions and/or access privileges.

All individuals with access to Twin Falls School District technology and computer networks will:

1. Respect the rights and property of others and will properly access files, data, or information of others.
2. Observe Twin Falls School District codes of conduct.
3. Utilize the computers, network, Internet, and other technologies only for purposes in support of the district's stated education goals or for legitimate school district business.
4. Be responsible for taking precautions to prevent loss or damage to equipment and data.
5. Install and use software on the district's computers only in accordance with Software Policy and Procedure Guidelines.

Interpretation, application, and modification of this use policy are within the sole discretion of the Twin Falls School District. Any questions or issues regarding this policy should be directed to the building or district administration, or the network administrator(s).

Software Policy and Procedures

Purpose: The Twin Falls School District licenses the use of computer software from a variety of third parties. The software developer normally copyrights such software. Unless expressly authorized to do so, the Twin Falls School District has no right to make copies of the software except for backup or archival purposes. The purpose of this policy is to prevent copyright infringement and to protect the integrity of the Twin Falls School District's computer environment from viruses and similar threats.

Policy and Procedures Guidelines: It is the policy of Twin Falls School District to respect all computer software copyrights and to adhere to the terms of all software licenses to which the district is a party. The Director of Operations is charged with the responsibility of monitoring these guidelines and will appoint school software managers. Twin Falls School District employees may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless the Twin Falls School District is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject employees, students, and/or the district to both civil and criminal penalties under the United States Copyright Act. Employees may not give standalone software to any other employee or any software to non-employees including parents, contractors, students, and others. Twin Falls School District employees and students may use software on local area networks or on multiple machines only in accordance with applicable license agreements.

Acquisition of Stand-Alone Software: To purchase and utilize software within the Twin Falls School District, employees must obtain the approval of their supervisor or school software manager. All software utilized by employees of the Twin Falls School District must be registered with the school software manager. Software acquisition channels are restricted to ensure that the Twin Falls School District has a complete record of all software that has been purchased for district computers and can register, support, track, and upgrade such software accordingly. All software will be subject to review and approval by the Twin Falls School District Curriculum Committee and Technology Department.

Acquisition of District-Wide Software: In order to facilitate the selection and implementation of software for use district-wide, a committee of district staff will be utilized to analyze and evaluate software packages. The committee participants will include staff members from each affected location and be lead by the Director of Operations, as to ensure that the selection best meets the needs of the district. Software selection is formalized to ensure a consistent process. To further ensure reliability and thoroughness, solution evaluations will be performed consecutively and FIFO (first-in-first-out) under normal circumstances. Because of time and scheduling demands, the committee will carefully screen each request for evaluation before committing to the research stage. Prioritization of evaluations may be modified at the discretion of the Director of Operations. The Director of Operations may elect to be the project manager for an evaluation project, or assign a committee member to be the project manager. At all stages, factors such as user reaction, effect on workload and efficiency for users and support personnel, and resources required should be considered.

Stage 1: Introduction of Need or Idea

Introduction of a software package, an idea, or recognized need will be formally presented to the evaluation committee during meetings with allowing agendas. The presenter should contact the Director of Operations to be scheduled. It is best if the presenter has done prior research, although presenting a solid idea may be sufficient. The presentation should include a justification and address an issue or need. A successful and effective presentation may include the following: available solutions, associated costs, source of funding, and research data such as product reviews and testimony.

Stage 2: Feasibility Analysis

The evaluation committee will perform an analysis of the presented data to determine whether or not to proceed with solutions research. This may be determined immediately after the initial idea presentation through discussion, or the Director of Operation may assign committee members to gather more data for analysis. Determination of initial and ongoing costs should be examined, and the availability of funding should be considered. If the committee decides the idea is feasible to research, it will be passed to the research subcommittee as assigned by the Director of Operations. A project manager may also be chosen to guide the process.

Stage 3: Research

It will be the responsibility of the research committee to gather the information and solutions to be compared. Any alternatives available should be considered. This committee will work with the curriculum committee, if necessary, to determine district curriculum standards compliance. The research committee will also work with the technology department to determine compatibility with the computers and networking systems in the district.

Stage 4: Evaluation and Testing

The solutions selected by the research committee will be evaluated and tested. All evaluation committee members will work with and evaluate the software, then report their findings to the project manager and committee in the format selected by the project manager. The information will be gathered according to timelines set by the project manager, then compiled for final review.

Stage 5: Finalization of Selection

Evaluation results will be discussed, and a final decision will be made. A solution may be selected for acquisition, or all evaluated solutions may be rejected. Final details regarding acquisition will be determined. This should include all necessary components, including software, hardware, and training. Determination of initial and ongoing costs will be finalized, as well as the source of funding. A system for technical support will be determined.

Stage 6: Deployment & User Training

The project manager will schedule the hardware and software deployment with the technology department. User training will be completed, and the technical support system will be established.

Stage 7: Gathering Feedback

After the software has been in use for a period of time, the project manager should gather data from the end-users regarding software and training effectiveness. This information can be used to improve the selection process.

Registration of Software: The district will register every software package. When a staff member acquires new software for use on district computers, he/she must inform the building software manager. The staff member should provide a copy of the registration to the building software managers. Software must be registered in the name of the district and department/school in which it will be used. Because of personnel turnover, software should never be registered in the name of the individual user. The software managers shall maintain a register of all of the district's software and shall keep a library of software licenses. The register will contain:

- the title and publisher of all software;
- the date and source of software acquisition;
- the location of each installation;
- the name of the authorized user;
- the existence and location of media ;
- the software product's serial number.

Storage and Security: The software managers shall be in charge of storing all district software in secured storage areas, if feasible. By ensuring secure storage of original media, the risk of software theft and unauthorized duplication of software is minimized.

Installation of Software: After the registration requirements above have been met, the software may either be installed by the school software manager or qualified individuals with the manager's permission. No software shall be installed on district computers without approval of the school software manager. Teachers who bring in data media from home are responsible to ensure that his or her media are free from viruses. District virus protection software should be used to examine these media before they are used in a district computer. These standards are to ensure that the district does not violate copyright laws or infect computer systems with viruses. A student shall not install computer software, bring in media from home, or tamper in any way with district software unless under direct supervision by a TFSD #411 staff member and only with approved software. It is the responsibility of teachers and other faculty members to constantly monitor student use of computers and review all policies and procedures with the students regarding the acceptable use of technology.

Documentation: Original manuals, tutorials, and other user-oriented documentation will be made available, whenever possible, to assist the software users. The district's trainers will also continue to provide in-service for teachers in the use of appropriate computer software.

Home Computers: The Twin Falls School District's computers are district assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on district machines. Generally, district owned software cannot be taken home and loaded on an employee's computer if it also resides on the district's computer. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. Before taking any software home, please check with the school software manager and follow the sign-out and sign-in procedures.

Software Audits: The school software manager will conduct random audits of all district PCs to ensure that the district is in compliance with all software licenses. During these random audits the district will search for inappropriate software and eliminate any that is found.

Software Log: A software log will be maintained of all software owned or used by the district. After the audit has been completed, the software log will be used to list all old and newly acquired software.

Penalties and Reprimands: Anyone who violates this policy will be referred to district administration for possible disciplinary action.

Policy Review: This software policy will be reviewed annually with staff. This software policy shall be updated as deemed necessary by the Twin Falls School District #411 Board of Education.

Hardware Policy and Procedures

Property Rights: The Twin Falls School District has the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment purchased or received by way of grant by a school or the district will be the property of the district. The district or school will determine the use. In accordance with grant specifications, neither employees, volunteers, nor students in the school have ownership rights to any equipment loaned to them by the school. Use of school equipment and software for private or personal business is strictly prohibited and will subject the violator to disciplinary action.

No person will have exclusive use of school equipment unless authorized by district administration.

Acquisition: Before acquiring new computers or computer-related equipment, each employee will consult with his or her building technician to ensure compatibility with the district's computer and network platform.

Network Attached Devices: Use of network attached devices, including, but not limited to, computers, printers, and handheld devices, must be approved by the building technician to ensure the compatibility, stability, and security of the district network.

Wireless Devices: Use of wireless equipment must be approved by the building technician to ensure the compatibility, stability, and security of the district network. To ensure that security standards are met, wireless devices will not be used until configured appropriately by district technology personnel. Any wireless device deemed to be a security liability will not be allowed. Random scans for rogue wireless devices may be performed by district technology personnel.

Enforcement: The District and all schools in the district will rigorously uphold laws pertaining to the use of technology equipment and the information contained in them and/or generated by its use. Anyone found to be violating such laws would be subject to suit for civil damages as well as prosecution by the school to the full extent of the law.

Electronic Network Use Rules

Every user (which includes, but is not limited to students, employees, volunteers, and contractors employed by the district) has the responsibility to respect and protect the rights of every user in our community and on the Internet. School district account holders are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use, and the laws of the state and the United States. Students will be provided with a school atmosphere and procedures of student control/discipline that will assure a suitable learning environment, and students will learn to act as responsible and productive citizens with respect for civil rights and the role of the individual in a democracy.

Using the network is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. Unacceptable conduct includes, but is not limited to, the following:

- Using the network for any illegal activity, including violation of copyright or other contracts.
- Using the network for financial or commercial gain.
- Using the network while access privileges are revoked or suspended.
- Degrading or disrupting equipment or system performance.
- Vandalizing the data of another user.
- Theft or plagiarism of data.
- Wastefully using finite resources.
- Unauthorized downloading of software.
- Gaining unauthorized access to resources or entities.
- Willfully and knowingly accessing or attempting to access pornographic or other inappropriate sites.
- Invading the privacy of individuals.
- Using an account owned by another user without authorization.
- Posting personal communications without the author's consent.
- Posting anonymous messages.
- Placing of unlawful or unlicensed information on a system.
- Using abusive or otherwise objectionable language in either public or private message.
- Sending of messages that are likely to result in the loss of recipients' work or systems.
- Sending of chain letters or broadcast messages to lists or individuals, or any other type of use that would cause congestion of the networks or otherwise interfere with the work of others.

Acceptable Posting: The Twin Falls School District provides a public Internet presence to share information with the community. Staff members are allowed to use these district provided resources and are responsible for monitoring and reviewing all content created by students. Students are not allowed to directly publish information to the public Internet via the school district network. Staff members agree not to publicly publish through the school district site any information that 1) violates copyright laws or property rights, 2) discloses student personal information other than names, 3) discloses student names with photographic depictions, 4) contains deliberately false or misleading statements regarding the school district, 5) are illegal, 6) are deliberately offensive, threatening, or libelous, or 7) are pornographic or otherwise obscene.

False Entry/Alterations: No student, volunteer, or school/district employee will make any false entry or alteration of any document, (either paper or electronic) used or intended to be used in connection with the operation of the Twin Falls School District nor any school in the district, nor will any student open or alter official school documents or private documents, either paper or electronic.

Data Security: The District assumes no responsibility or liability if documents stored on school equipment are lost or damaged, nor will the district be responsible for security violations beyond the appropriate punishment of those persons involved in such violations.

Controlled Access to the Internet: Internet access is provided strictly for use consistent with the district's educational and business goals. It is the practice of the Twin Falls School District to protect staff and students from obscene, pornographic, and other inappropriate material available on the Internet by monitoring Internet access and by using mechanisms such as content filters and firewalls in accordance with the Children's Internet Protection Act. Students are not allowed to access the Internet without staff supervision and are required to connect to the web through a content filter. Attempts to access inappropriate material are logged. Deliberate attempts to access obscene or inappropriate materials by any user will result in disciplinary action by school district administration. The school district may provide direct communication systems such as e-mail or chat rooms for student use, which will be either filtered for content, closed (in-district only), or both. To provide student safety and security, the use of Internet direct

communication systems is allowed only under direct staff supervision. Web-based direct communication systems pass through a content filter.

Unlawful and Unauthorized Activities: The Twin Falls School District does not tolerate the use of the network for illegal activity, including electronic crimes such as unauthorized access, deliberate use of malicious code such as viruses, and deliberate attacks on systems (“hacking”). These activities will result in disciplinary action by school district administration.

Network Etiquette

- Be polite. Do not get abusive in your messages to others.
- Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language.
- Exercise caution with personally identifiable information. Do not reveal personal information of others. Any student receiving unsolicited requests for personal information will immediately report that to the supervising teacher. That teacher will report this incident to appropriate authorities.
- Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to authorities.
- Do not use the network in such a way that you would disrupt the use of the network by other users.
- Information accessible via the network and Internet should be assumed to be private property and possibly copyrighted.

Enforcement

Violation of the rules set forth by school district policy may result in disciplinary action by school district administration. Systems managers may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of information technology resources. Disciplinary action for misuse by students may include, but is not limited to, suspension from school, removal from classes requiring computer use, loss of computer use privileges, and, if deemed appropriate, criminal prosecution. Disciplinary action for misuse by employees and other users may include, but is not limited to, formal reprimand, probation, termination, and, if deemed appropriate, criminal prosecution. School district administration and system managers will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final. Before any permanent action is taken against a user, the user will be advised of the bases for the proposed action and given an opportunity to respond. The specific disciplinary action for each case will be at the sole discretion of school district administration and may vary depending on the severity of the infraction.

Security

Security on any computer is a high priority. Do not use another individual’s account without written permission from that individual. Attempts to log onto the network with another person’s identification without permission may result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the computers and network. If you feel you can identify a security problem on the network, you must notify an administrator.

Policy Agreement

The Twin Falls School District will uphold laws pertaining to the use of information technology equipment and the information contained therein and/or generated by its use. Anyone found to be violating such laws would be subject to suit for civil damages as well as prosecution to the full extent of the law.

There is a need for full disclosure and understanding for the partnership between parents, children, and the school district in regard to technology and its use. A Computer and Network Use Agreement has been

created to inform and provide knowledge, ensuring that all parties understand the areas of responsibility identified. Each child will need to have an agreement form signed and on file before the student will be allowed to use the computers.

Warranties/Indemnification

The District believes that the benefits to educators and students from access to the Internet (in the form of information resources and opportunities for collaboration) far exceed any disadvantages of access. Ultimately, parent(s) and guardian(s) of minors are responsible for their child's behavior, and this includes use of the Internet.

The District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s)/legal guardian(s) agrees to cooperate with the District in the event of the school's initiating an investigation of a user's use of his/her access to its computer network and the Internet.

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 these procedures.

Legal Reference: Children's Internet Protection Act, P.L. 106-554
20 U.S.C. § 6801, et seq.
47 U.S.C. § 254(h) and (1)

Promulgated on: May 2001
Revised: May 2004
Revised: November 2005

Twin Falls School District #411 Computer and Network Use Agreement

201 Main Avenue West
Twin Falls, Idaho 83301

Telephone: 208-733-6900
Fax: 208-733-6987



School district computer users are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the networks they use, and the laws of the state and the United States.

The computers and network are provided for furthering the District's stated educational goals only, and they are to be used by authorized individuals only. Individuals using these systems are subject to having all activities on these systems monitored by system or security personnel. Anyone using these systems expressly consents to such monitoring.

It is possible for all users of the Internet, including your child, to access information that is intended for adults. Although the District has taken reasonable steps to ensure that the Internet connection is used only for purposes consistent with the curriculum and that inappropriate sites (as defined by the Children's Internet Protection Act) are filtered, the district or school cannot entirely prevent the availability of inappropriate material elsewhere on the Internet.

It is possible that a determined user may make use of computer resources for inappropriate purposes. Deliberate misuse of the computer network or the Internet may result in disciplinary action as outlined in the Computer and Network Use Policy.

I, _____ and _____
Parent Name (please print) Student Name (please print)

have read the Computer and Network Use Policy, understand it, and agree to adhere to the principles and procedures detailed within. We understand and accept the conditions stated above and release from any liability the Twin Falls School District #411 (the sponsoring school), its subcontractors, and employees.

I understand that my child is expected to use good judgment and follow the guidelines of the Computer and Network Use Policy. Furthermore, I have discussed the information contained in the Computer and Network Use Policy with my child. Should my child breach the policy guidelines, I understand that my child may lose privileges on the Twin Falls School District computer network or be subject to other disciplinary action.

Parent Signature

Student Signature

Date

May 2004