Redford Union School District #1

Policy #5801

ACCEPTABLE USE POLICY
USE OF TECHNOLOGY AND ELECTRONIC RESOURCES

The Board of Education recognizes that it is important for students to have access to electronics-based resources and master skills for their application to learning, problem solving, production of work, and the processing and presentation of information. The Board also recognizes that while these resources represent extraordinary learning opportunities and enriching educational materials, they also offer persons with illegal or unethical motives avenues for reaching those using resources. Additionally, these resources present tempting opportunities for users to explore areas that are either confidential, have restricted access or are inappropriate to the classroom or workplace. It is the policy of the Board of Education that the use of the technology and electronic resources of the Redford Union School District shall in all respects conform to and comply with applicable state and federal laws or regulations and shall be appropriate for our educational purpose and programs for students. It shall be the responsibility of the Superintendent of Schools and administrative staff of the School District to implement the Administrative guidelines.

Redford Union School District #1

ADMINISTRATIVE PROCEDURE: 4150 Adopted: January 20, 2012

ADMINISTRATIVE GUIDELINES

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC RESOURCES

Preamble

The Redford Union Schools District provides access to technology resources including access to the Internet. These resources allow interaction internally within the district and externally to systems located all over the world. These resources have a limited educational purpose. This purpose is to provide access to electronic resources to promote and enhance students, staff and board member learning, consistent with district educational goals and objectives. This acceptable use policy ensures that use of the network by students and staff and board members is done in an appropriate manner. Network use is a privilege and not a right. Users are obligated to respect and protect the rights of every other user and act in a responsible, ethical and legal manner. Failure to abide by this policy may result in loss of privileges, disciplinary action and or legal action, as described in the "Consequences & Disciplinary Action" section below.

District Resources

District technology resources consist of any two-way interactive communication device and voice/video, data, such as, but not limited to, telephones, computer hardware, computer software, district provided email addresses, communication lines and devices, graphing calculators, terminals, printers, CD-ROM devices, scanners, digital cameras, LCD projectors and any other technology devices. District electronic resources may consist of any electronic resource accessed by a user, including, but not limited to, the internet, including all online databases, programs, and features; electronic mail; online discussion groups; wikis; online chats; online forums; and all other electronic communication features.

Internet Safety Measures

The Superintendent shall be responsible for directing appropriate District technology staff, to bring all computers used by children and adults into full compliance with all federal requirements regarding Internet filtering software to assure that District discounts for Internet access and internal connections under the federal E-rate program are not jeopardized.

Student Internet activities will be monitored by the District to ensure that students are not accessing inappropriate sites. Each District computer with Internet access shall have a filtering device or software that locks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors.

Staff and Board Member, District internet and intranet activities may also be monitored to ensure compliance with the District's acceptable use policy, guidelines and the law and may also be searched and downloaded as part of the District's records.

Acceptable Use

The Superintendent of Schools shall determine the persons appropriate for use of the technology and electronic resources of the School District. Written procedures shall be developed for the determination and authorization of those persons for use of the technology and electronic resources of the School District in conformance with the Acceptable Use Policy of the Board of Education, Policy #5801 and the requirements of these guidelines. Those persons so authorized shall be referred to as "authorized individuals" hereafter in these guidelines. All authorized individuals shall be required to read, sign and submit the USER ACKNOWLEDGEMENT AND CONSENT FORM contained in Part X of these Administrative Guidelines prior to any use of the technology and electronic resources of the School District.

One fundamental need for acceptable use of School District electronic resources is respect for, and protection of, password/account code security, as well as restricted databases, files and information banks. Personal passwords/account codes shall be created to protect authorized individuals utilizing electronic resources to conduct research or complete work.

When using the School District's internet, email, or technology and/or the School District's electronic resources outside of school in ways that may impact the school community, students, staff and board members are expected to demonstrate the same courtesy and respect towards members of the community that they are expected to show at school. The school reserves the right to take disciplinary action, as outlined in the "Consequences & Disciplinary Action" section below, in cases where out-of-school use of the School District's internet, email, or technology and/or the School District's electronic resources has an impact on the school community or learning or work environment.

Authorized individuals having access to School District technology and electronic resources must consistently maintain a high degree of personal responsibility. The use of School District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges and could lead to additional disciplinary action as described in the "Consequences & Disciplinary Action" section below. Each authorized individual who receives a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account may be suspended or closed, and further disciplinary action may be taken, pursuant to the "Consequences & Disciplinary Action" section below, upon the finding of misuse of School District technology and electronic resources by the authorized individual.

These passwords/account codes shall not be shared with others; nor shall authorized individuals use another person's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects authorized individuals from wrongful accusation of misuse of electronic resources or violation of School District policy, state or federal law. Access to technology and electronic resources are a limited and expensive resource.

Authorized individuals are allowed to conduct network-based activities which are instructional or directly related to job performance as described and/or directed by the School District. Use unrelated to instruction or job performance ("personal use") shall comply with all applicable rules allowing such use and shall be prohibited in the absence of any rule allowing such use. Any rules allowing personal use will in no way interfere with the instructional or professional computer time and use for which the hardware and software are intended. Authorized individuals who misuse electronic resources or who violate laws may be, in addition to the loss of privileges, subject to disciplinary action as described in the "Consequences & Disciplinary Action" section below.

The use of the School District's technology and electronic resources are a privilege, which may be revoked at any time. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of another person's right to privacy; using another person's name to send or receive messages on the network; sending or receiving unauthorized personal messages; and use of the network for personal gain, commercial purposes or to engage in political activity for any candidate or proposition. In no event may the District's technology and electronic network system be used for non-instructional or non-work related purposes while on the job unless otherwise permitted herein.

Authorized individuals may not claim personal copyright privileges over files, data or materials developed by use of School District equipment or resources, nor use copyrighted materials without the permission of the copyright holder. Even though it is possible to download most materials authorized individuals shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (email) is a privilege and designed to assist authorized individuals in the acquisition of knowledge and in efficiently communicating with others. The School District email system is designed solely for instructional and job performances purposes. Email chain letters, online discussion groups, wikis, online chats, online forums, and other electronic communications features are not allowed, with the exception of those that are created by teachers or instructors for specific instructional purposes or by employees for specific work related communication. All use of email or the internet that is not related to instruction or job performance is prohibited and subject to disciplinary action as described in the "Consequences & Disciplinary Action" section below. Additionally, School District administrative personnel may access and read any and all information (**including system histories**) transmitted or posted by users via email, or the internet, including, but not limited to, discussion groups, wikis, chats, forums and other electronic communication features. Furthermore, by posting messages, uploading files, inputting data or engaging in any other form of communication through these applications a user grants the School District permission to use, modify, copy, distribute, transmit, publicly display, reproduce, and publish any such communication. The use of personally owned technology while on the job is subject to this policy and these guidelines and otherwise may only be used during authorized breaks or for emergency communications or legal, policy and guideline compliant communications that can only be reasonably conducted at such times.

Failure to abide by the Acceptable Uses described above may subject a user to consequences and/or disciplinary action as described in the "Consequences & Disciplinary Action" section below.

Unacceptable Uses

Authorized users who engage in investigatory activities commonly described as "hacking" are subject to loss of access privileges and discipline as described in the "Consequences & Disciplinary Action" section below. "Hacking" includes the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the School District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, authorized individuals are not permitted to obtain download, view or otherwise gain access to materials, which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise prohibited under School District policy, guidelines or rules.

The School District administrative personnel reserves the right to review or remove files, limit or deny access, and refer authorized individuals for consequences and/or disciplinary action as described in the "Consequences & Disciplinary Action" section below.

Network Etiquette & Privacy

Authorized individuals are expected to abide by the generally accepted rules of electronic network etiquette for system users. These include, but are not limited to, the following:

1. System users must be polite. They may not send abusive, insulting, harassing, or threatening messages to others.

2. System users must use appropriate language. Language, which uses vulgarities or obscenities, libels others, or uses hostile, or discriminator epithets or references, is prohibited.

3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, volunteers or other individuals during email transmissions.

4. System users may not use the School District's electronic network in such a manner that would damage, disrupt or prohibit the use of the network by other users.

5. System users must assume that all communications and information is public when transmitted via the network and may be viewed by other users or monitors. School District Administrators may access and read email on a random basis to monitor appropriate use..

6. System users are prohibited from use of the School District's electronic network for unlawful purposes and such use will not be tolerated.

7. System users must immediately report to their immediate supervisor/administrator any violation of the District's acceptable use policy or guidelines.

Failure to abide by the generally accepted rules of electronic network etiquette may subject users to consequences or disciplinary action as described in the "Consequences & Disciplinary Action" section below.

Waiver of Warranty/Disclaimer

While the School District is providing access to electronic resources, it makes no warranties of any kind, whether expressed or implied, for the services it provides. The School District may not be held responsible for any damages suffered by any person while using these services. These damages include loss of data as a result of delays, non-delivery, missed delivery or service interruptions caused by unforeseen network problems or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The School District specifically denies any responsibility for the accuracy of information obtained through Internet services.

The District does not guarantee that materials stored on the system will be private. Network administrators may review the information stored on the system to determine whether it is being used properly.

Security

The Board of Education recognizes that security on the School District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges create a risk for all users of the information system. The account codes and passwords provided to each user are intended for the exclusive use of that person. Any problems which arise from the users sharing his/her password/account are the responsibility of the account holder. Any misuse, including the use of an account by someone other than the registered holder, may result in the suspension or revocation of account privileges and other consequences or disciplinary action as described in the "Consequences & Disciplinary Action" section below.

All authorized individuals are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the teacher or school district administrator.

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm or destroy equipment or data of another user, the School District information service, or the other networks that are connected to the Internet, whether successful or not. This includes, but is not limited to, the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the School District electronic network or technology system will result in the immediate loss of access privileges and other consequences and/or disciplinary action as described by the "Consequences & Disciplinary Action" section immediately below.

Consequences & Disciplinary Action

The consequences and/or disciplinary action for any user violating the School District's Acceptable Use Policy, Administrative Guidelines or any rules or procedures issued pursuant to the policy or guidelines for acceptable use, include but are not limited to one or more of the following:

- Suspension of network privileges
- Revocation of network privileges
- Suspension of Internet access
- Revocation of Internet access
- Suspension of computer access
- Revocation of computer access
- Restitution for replacement cost, cost for repair, cost of technician time
- Consequences pursuant to the Student Handbook (students only)
- Suspension from school (students only)
- Expulsion from school (students only)
- Disciplinary action up to and including dismissal (employees & volunteers only)
- Referral to law enforcement authorities for prosecution

REDFORD UNION SCHOOLS

ACCEPTABLE USE OF TECHNOLOGY AND ELECTRONIC RESOURCES

EMPLOYEE'S SIGNATURE PAGE

X. USER ACKNOWLEDGEMENT FORM

I, _____, as an authorized individual user in the Redford Union School District, acknowledge that I have read the School District's Acceptable Use Policy and Administrative Guidelines and will comply with them. In addition, I acknowledge that the School District may review the electronic mail (email) files or messages sent to or received by me, using the School District's computer equipment or networks, etc., and hereby consent to the review of my electronic mail files by the School District's Administration personnel to monitor my compliance with the Acceptable Use Policy and Administrative Guidelines.

_____
Name (please print)

_____
Building

_____
Signature Date