

Computer, E-Mail, Internet, and Information Technology Acceptable Use Policy

I. Definitions

As used herein:

A. "User" means all persons who are granted access to the School District's computer resources.

B. "Computer Resources" means all computer hardware, computer software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals and guides.

II. No Expectation of Privacy

A. No expectation of privacy. The computers and computer accounts given to Users are to assist them in performance of their jobs. Users do not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the School for business and/or education program purposes.

B. Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allowing personnel of the School 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 School may use human or automated means to monitor use of its computer resources.

III. Prohibited Activities

A. Inappropriate or unlawful material. Material that is fraudulent, harassing, embarrassing, lewd, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensively proselytizing inappropriate or otherwise unlawful, or in violation of School Board policy may not be sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

B. Prohibited uses. Without prior written permission from the District's Technology Coordinator, computer resources may not be used for dissemination or storage of commercial or personal advertisements, promotions, destructive programs (including but not limited to self replicating codes or viruses), political or religious material, receipt or distribution of inappropriate or unlawful material as defined above, participation in or accessing chat lines, chat groups or chat sites (unless directly related to the school curriculum and such access has been authorized in advance by the building supervisor or Director of Computer Resources), accessing any site which displays or distributes inappropriate or unlawful material as defined above, or any use which is unauthorized or in violation of School Board policy.

C. Waste of computer resources. Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending or forwarding mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, sending or forwarding jokes, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

D. Misuse of software. Without prior written authorization from the School's Technology Coordinator, Users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any third person; (3) install software on any School workstations or servers; (4) download any software or run executable files from the Internet, email or other online service to any School's workstations or servers; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their supervisors.

E. Communication trade secrets. Unless expressly authorized by the School's Technology Coordinator, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the School is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996.

IV. Passwords

A. Responsibility for passwords. Users are responsible for safe-guarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

B. 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 School has global passwords that permit it access to all material stored on its computer system-regardless of whether that material has been encoded with a particular User's password.

V. Security

A. Accessing other 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 the computer system to "snoop" or pry into the affairs of other users or School operational systems by unnecessarily reviewing their files and e-mail without authority.

B. Accessing other computers and networks . A User's ability to connect to other computer systems through the network 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.

C. Computer security. Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of School Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the District's network via Internet connections or by leaving systems on and logged into the network without authorization and to prevent the introduction and spread of viruses.

VI. Viruses

Virus detection. 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 School's network. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to School MUST be scanned for viruses and other destructive programs before being placed onto the computer system or network. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to School's network MUST be scanned for viruses.

VII. Encryption Software

A. Use of encryption software. Users may not install or use encryption software on any of the School's computers without first obtaining written permission from their supervisors. Users may not use passwords or encryption passwords that have not been provided to their supervisors.

B. Export restrictions. The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in any way outside the United States without the prior written authorization from the School's Technology Coordinator.

VIII. Miscellaneous

A. Compliance with applicable laws and licenses. In their use of Computer Resources, Users must comply with all software licenses; copyrights; all other state, federal, and international laws governing intellectual property and online activities.

B. Other policies applicable. In their use of Computer Resources, Users must observe and comply with all other policies and guidelines of the School.

C. Computer configuration. The following items are considered user configurable and may be changed by the operator; screen saver, mouse pointers, additions to the Word Perfect power bar that do not replace the office standard, views in mail, Vision or Word Perfect. Manipulating computer configuration

items not in this list may be subject to disciplinary action if not authorized by the School's Technology Coordinator.

D. Amendments and revisions. This policy may be amended or revised from time to time as the need arises. Users shall comply with all amendments and revisions once adopted by the School Board.

E. No additional rights. This Policy is not intended to, and does not grant, Users any contractual rights. **IX.**

Violation/Consequences

A. Students.

1. Students who violate this policy shall be subject to revocation of district system access up to and including permanent loss of privileges, and discipline up to and including expulsion.
2. Disciplinary action may be appealed by parents and/or students in accordance with existing district procedures for suspension or revocation of student privileges.

1. Staff who violate this policy shall be subject to discipline, up to and including suspension, termination or discharge, in accordance with Board policy, negotiated agreements and applicable law.

C. Violations of law: Violations of law by students or staff will be reported to law enforcement officials

SCHOOL DISTRICT INFORMATION TECHNOLOGY CODE OF CONDUCT

Use of the School District's Information Technology Systems, including all computer hardware, computer software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals and guides, by students and staff of the Questa Independent School District shall be in support of education and research that is consistent with the mission and curriculum of the School District. Internet use is limited to those persons who have been issued district approved accounts.

Use will be in accordance with the district's Acceptable Use Procedures and this Code of Conduct:

1. Keep confidential and protect all computer and Internet passwords, access codes or logon information from disclosure to others.
2. Respect the privacy of other users. Do not use other users' passwords. Unauthorized use of passwords, access codes or other confidential account information may subject the user(s) to discipline, and to both civil and criminal liability.
3. Be ethical and courteous. Do not send hate, harassing or obscene mail, discriminatory remarks, or demonstrate other antisocial behaviors. State law prohibits the use of electronic communication facilities to send fraudulent, harassing, obscene, indecent, profane, intimidating or other unlawful messages. See NMSA 1978, § 30-451 et seq
4. Maintain the integrity of files and data. Do not modify or copy files/data of other users without their consent.
5. Treat information created by others as the private property of the creator. Respect copyrights. Software protected by copyright shall not be copied except as licensed and stipulated by the copyright owner.
6. Use the network in a way that does not disrupt its use by others. Do not use the Internet for commercial purposes. Transmission of commercial or personal advertisements, solicitations, promotions, destructive programs or other unauthorized use unrelated to the mission or curriculum of the School District is prohibited.
7. Do not destroy, modify or abuse the hardware or software in any way.

Users shall report any suspected abuse, damage to equipment or tampering with files to the School District system operators.

8. Do not develop or pass on programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system, such as viruses, worms, "chain" messages, global mailings, ResEdit, etc. Do not "hack" the system. Attempts to gain unauthorized access to confidential information or private directories maintained by the School District or to circumvent privacy protections on internal files or non-public restricted files, accounts or directories of any external source is a violation of this code of conduct, and may subject the user to civil or criminal liability.
9. Do not use the Internet to view, access, download or process pornographic, obscene, indecent, profane or otherwise inappropriate material.
10. Use of the system to access games and use of computer time for game-playing shall be restricted solely to instances directed and monitored by instructional staff and is limited to games which address educational goals.

In addition to disciplinary sanctions which the School District may impose upon students or staff under applicable policies, codes of conduct or administrative regulations, the District reserves the right to remove a user's account and deny use and access of the computer system if it is determined that the user is engaged in unauthorized activity or is violating this code of conduct.

Student Information Technology Access Release Form

As a condition to use of the School District's Information Technology Systems, including all computer hardware, computer software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals and guides, I understand and agree to the following:

1. To abide by the School Board's Acceptable Use Policy and its Information Technology Code of Conduct.
2. That the Questa School District administrators have the right to review any materials created or stored in any files I may create and to edit or remove any material which they, in their sole discretion, believe may be unlawful, obscene, abusive, or otherwise objectionable and I hereby waive any right of privacy which I may otherwise have to such material.
3. That the Questa School District will not be liable for any direct or indirect, incidental or consequential damage due to information gained and/or obtained via use of the School District's computer system including, without limitation, access to public networks.
4. That the Questa School District does not warrant that the functions of the School District computer system or any of the networks accessible through the system will meet any specific requirements you may have, or that the School District Information Technology Systems will be error-free or uninterrupted.
5. That the Questa School District shall not be liable for any direct or indirect, incidental, or consequential damages (including lost data or information) sustained or incurred in connection with the use, operation, or inability to use the School District's Information Technology Systems.
6. That the use of the Questa School District Information Technology Systems, including access to public computer networks, is a privilege which may be revoked by School District administrators at any time for violation of the District's Acceptable Use Policy or Information Technology Code of Conduct. School District administrators will be the sole arbiter(s) of what constitutes a violation of the Acceptable Use Policy or Code of Conduct.

7. In consideration for the privilege of using the School District's Information Technology Systems, and in consideration for having access to the public networks, I hereby release the Questa School District, the School Board, its members, administrators and employees, including its computer operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use, or inability to use, the School District Information Technology Systems.

Printed Name of Student User: _____

School: _____ Grade: _____ Student ID: _____

I hereby certify that I will abide by the conditions set forth in this document, the School District's Acceptable Use Procedures and Computer and Internet Code of Conduct.

Signature of Student User

Signature of Parent/Guardian

Date: _____

Date: _____

To be signed by authorized staff member.

I certify that the above parents and student have received a copy of the School Board Computer, EMail, Internet, and Information Technology Acceptable Use Policy and the Information Technology Code of Conduct.

Printed Name

Signature

Date: _____

Date: _____