



RULES FOR STUDENT USE – SUMMARY

- QDA equipment and network resources are to be used for educational purposes only.
- All electronic traffic created or transmitted on QDA property is monitored, logged, and subject to review to ensure compliance with this guideline.
 - This includes all Internet traffic, email messages, and programs installed on QDA computer systems.
- All electronic data that passes through a QDA owned computer system or over QDA's network is subject to monitoring and seizure and may be handed over to law enforcement officers.
- QDA may hold users (or their legal guardian) personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred, and any costs incurred to return such services to their normal state.
- Users are bound to the full agreement whenever they access the QDA Network or uses QDA-owned equipment.

Users are expected to review the full guideline in its entirety on a yearly basis.

COMPUTER NETWORK / INTERNET MANAGEMENT AND ACCEPTABLE USE

RULES FOR STUDENT USE

Users consent to the terms of this guideline whenever he or she accesses the QDA Network or uses QDA Equipment. Users of the Network are bound to the terms of this Agreement regardless of whether or not a copy was received and/or signed for by the User.

QDA recognizes that an effective educational system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, QDA will use technology resources as a powerful and compelling means for students to learn core subjects and apply skills in relevant and rigorous ways. It is QDA's goal to provide students with rich and ample opportunities to use technology for important purposes just as individuals in workplaces and other real-life settings. QDA's technology resources will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

Scope of this Agreement

This agreement applies to any action that creates traffic on the QDA network, including traces or remnants of traffic that pass through QDA equipment, wiring, wireless networks, or storage devices.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision. QDA will also have procedures or guidelines that provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA.

The procedures or guidelines will be designed to:

- Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the World Wide Web;
- Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

- Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and
- Restrict minors' access to materials "harmful to minors," as that term is defined in CIPA.

Pursuant to Federal law, students will receive education about appropriate on-line behavior, including: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors while interacting with other individuals on social networking websites, using e-mail, chat rooms, other forms of direct electronic communications, and cyberbullying awareness and response; (c) unauthorized access (e.g., "hacking") and other unlawful activities by minors on line; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

Parents should be aware that:

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take personal responsibility for his or her use of the network and Internet and avoid objectionable sites.
- Users/parents/guardians are advised that use of any network may include the potential for accessing web sites with inappropriate materials. It is the responsibility of all users to attempt to avoid these sites through prudent use of the Internet. If a student accidentally accesses one of these sites, they should immediately exit from that site and/or notify a staff member.
- Any attempts to defeat or bypass QDA's Internet filter or conceal Internet activity are prohibited, whether the attempt is made with QDA-owned equipment or a personal technological device on the QDA Network. The attempts include use of proxies, https, special ports, third party applications, modifications to browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.
- QDA is not responsible for students accessing information from personal mobile devices outside of the QDA network.

I. Personal Responsibility

By using the QDA Network or Equipment, you are agreeing not only to follow the rules in this guideline, but are agreeing to report any misuse of the network to the QDA Technology Department or your Instructional Supervisor. Misuse means any violation of this guideline, Board of Education Policy, or any other use that is not included in the guideline, but has the effect of harming another person or his or her property.

II. Terms of Permitted Use

By using the QDA Network or Equipment, the student acknowledges and understands the following regarding the use of the computer/network:

1. Computer use is not private. System managers have access to all messages including illegal activities and activities not in the best interest of QDA. Inappropriate and illegal activities may be reported to the authorities.
2. All electronic data that passes through a QDA owned computer system or over QDA's network is subject to monitoring and seizure and may be handed over to law enforcement officers.
3. All electronic data created for administrative or instructional purposes under the Board approved curriculum for a course or program is the property of QDA.
4. The rules and regulations of online etiquette are subject to change by the Administration. The Student Code of Conduct rules are applicable in the online environment as well.
5. The user in whose name a computer system is issued is responsible for its proper use at all times. Users must log off the computer to conclude a session or lock the computer if stepping away. Users retain responsibility for the activity of anyone accessing the computer and/or network under their account. Users shall keep personal account information, home addresses and telephone numbers private. They shall use this system only under the login and password information issued to them, by QDA. Users shall not grant others access to a computer and/or the network under their login and password.
6. Computer systems and the QDA network shall be used only for purposes related to education.
7. Violation of this guideline may result in the cancellation of user privileges and possible discipline under the Student Code of Conduct.

III. Acceptable Use

QDA is providing access to its computer network and the Internet for educational purposes *only*. If you have doubt about whether a contemplated activity is educational, you should ask your Instructional Supervisor or the technical support staff if a specific use is appropriate.

IV. Unacceptable Use

Among the uses that are considered unacceptable and which constitute a violation of this guideline are the following:

1. Violating or encouraging others to violate the law or Board Policy.
2. Revealing private information about yourself or others. Private information includes, but is not limited to a person's password, social security number, credit card number or other confidential information that has the potential to harm you or others or to violate the law if shared with other persons.
3. Uses that cause harm to others or that cause damage to their property.
4. Uses that constitute defamation (i.e. harming another's reputation by lies), or that harass, threaten or bully others.
5. Using profanity, obscenity or other language, which may be offensive to other users.

6. Uses that are for commercial transactions (i.e. buying or selling or making arrangements to buy or sell over the internet).
7. Use that causes disruption to the use of the computer and/or network by others or that disrupts the educational process of QDA.
8. Using the system to encourage the use of drugs, alcohol or tobacco.
9. Viewing, downloading or transmitting material that is threatening, pornographic, obscene, disruptive or sexually explicit or that could be construed as harassment or disparagement of others based on their race, national origin, citizenship status, gender, sexual orientation, age, disability, religion or political beliefs.
10. Copying or placing copyrighted material or software on the system without the author's permission and/or in violation of law.
11. Reading, deleting, copying or modifying other user's email or files without their permission or attempting to interfere with another user's ability to use technology resources.
12. Using another person's password or some other identifier that misleads recipients into believing someone other than you is communicating or accessing the network or Internet.
13. "Hacking," gaining, or attempting to gain unauthorized access to computers, servers, computer systems, internal networks, or external networks.
14. Use that causes excessive consumption of paper and other relevant supplies.
15. Downloading and/or installing freeware or shareware programs without the approval of the Technology Department. This includes use of peer-to-peer file sharing programs.
16. Uploading a worm, virus or other harmful form of programming onto the network or Internet.
17. Plagiarizing copyrighted or non-copyrighted materials for personal gain, recognition, or as graded work.
18. Using social network sites such as Facebook, Twitter, and others and/or forum sites and/or blog sites for the purpose of posting slanderous or otherwise harmful information, whether true or untrue, about the character and/or actions of the district's students or staff on district or personal technology equipment.
19. Uses that degrade or disrupt the operation of the Network or that waste limited computer, paper or telephone resources or cause unnecessary traffic. The System Administrator may also develop specific limitations on the use of graphics, the size, number, and type of attachments, and the overall size of e-mail messages sent on the system. The use of multiple messages, non-system addresses, or other techniques to circumvent these limitations is strictly prohibited.

V. Privacy

Network and Internet access is provided as a tool for your education. QDA reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the

QDA and no user shall have any expectation of privacy regarding such materials, regardless of storage location.

VI. Vandalism

Vandalism will result in disciplinary action that may include cancellation of privileges, suspension/expulsion and/or prosecution. Vandalism is defined as any malicious attempt to harm or destroy data of another user or equipment or any network connected to any of the Internet backbones. This includes, but is not limited to, the uploading or creation of computer viruses or spyware, erasing, deleting, or otherwise making the school's programs or networks unusable and includes theft or the damaging or defacing of equipment. QDA may hold users (or their legal guardian) personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs incurred, and any costs incurred to return such services to their normal state.

VII. Warranties/Indemnification

QDA makes no warranties of any kind, either express or implied, in the connection with its provision of access to and use of its computer networks and the Internet provided under this Guideline and Agreement. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Guideline and Agreement. The User takes full responsibility of his or her usage and agrees to indemnify and hold harmless QDA and its Board members, administrators, teachers, and staff from any and all loss, costs, claims, or damages resulting from the 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 and, if the user is a minor, the user's parent(s) or guardian(s) agrees to cooperate with QDA in the event of the initiation of an investigation into a user's use or his or her access to its computer network and Internet, whether that use is on a District computer or on another's outside QDA's Network.

LEGAL REFS.:

U.S. Const. Art. I, Section 8

Family Educational Rights and Privacy Act; 20 USC 1232g et seq.

Children's Internet Protection Act; (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)

ORC 1329.54 through 1329.67

3313.20

3319.321

Filtering and Monitoring Guidelines

1. QDA installs a third party application on all computer systems used by students for content filtering. This application is available upon request for use on a personal computer system. Please contact the QDA Technology Department for additional information.
2. Content filtering system protects against visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in CIPA.
3. Content filtering system restricts minors' access to materials "harmful to minors," as that term is defined in CIPA.
4. Content filtering system prevents unauthorized access, including so-called "hacking," and other unauthorized activities by minors online.
5. Content filtering system records web history for each computer system and the QDA Administration can review this information to ensure compliance.
6. Content filtering system automatically notifies the QDA administrations when user accesses or attempts to access inappropriate matter on the Internet and the World Wide Web.
7. To promote safety and security of minors, QDA has designated the following Internet Safety Policy to educate students (<http://lms.go2qda.org/policy/internet-safety.pdf>).