



ACCEPTABLE USE OF INTERNET AND NETWORK RESOURCES – 3.003-15

Overview – Posted Policy

1. **Email:** The QCS email system is established and maintained for the conduct of business, teaching and student access.

- a. Is only to be used for those purposes.
- b. Commercial, illegal, or immoral use of the email system is prohibited.
- c. QCS retains the right to monitor all email activity within legal limits.

2. **Internet access** is provided for all faculty, staff and students

- a. To be used for professional and education purposes only.
- b. Internet users are prohibited from using the QCS network to access, download, store, or transfer immoral, illegal or pornographic content.
- c. Using the internet connection in such a way that would impede the performance of the QCS network.

3. Computer and network security

- a. All users on the QCS network are required to use secure login passwords and secure screen savers.
- b. Users are prohibited from sharing their account login information including account names and passwords, except:
 - i. Student accounts will have their login information shared with parents/guardians and teachers to allow monitoring of their activity
- c. Students **MUST** use the provided student wireless network. Use of any other wireless network is strictly prohibited.
 - i. Use of any type of technology to bypass the QCS network is strictly prohibited.
 - ii. Students are not allowed to connect to the school network using wired connections.
 - iii. Students may not set up their own wireless access point including pairing with a personal wireless device (cell phone, tablet, etc.)

4. Internet Safety

- a. QCS employs filters to block online content, including:
 - i. Age-inappropriate content
 - ii. Illegal, immoral or obscene content
 - iii. Technically unsafe content
- b. Students are prohibited from attempting to bypass these filters by any means, including:
 - i. VPN connections
 - ii. Software
 - iii. Browser modifications
- c. Safety training will be conducted for all students
- d. Enforcement and consequences
 - i. Responsibility for notification
 - ii. Consequences

This document was approved by the QCS Board of Directors on Thursday, October 10, 2013. The document was modified July 21, 2021 to include the Overview page to improve clarity.



E-Mail

Quakertown Christian School ("QCS") maintains an electronic mail system. This system is provided by the school to assist in the conduct of its business and educational operations. All messages composed, sent, or received on the electronic mail system are and remain the property of QCS. These messages are not the private property of any employee or student of QCS.

The use of the electronic mail system is reserved solely for the conduct of QCS business and in the classroom as part of the instructional process.

By using the QCS electronic mail system, an employee or student agrees to be bound by this policy and to comply with all applicable local, state, and federal laws and regulations.

Internet

The following guidelines have been established for use of the Internet by QCS employees and students.

All communication and use should be for professional and educational purposes only. Employees and students are responsible for seeing that the Internet is used in an effective, ethical and lawful manner.

Employees and students are prohibited from using the Internet to visit, view, download, transfer, and store, disseminate or otherwise contact pornographic, sexually explicit, or other inappropriate sites, addresses, and/or websites. Employees and students are prohibited from using, storing, and making available any materials the possession or distribution of which is illegal. Likewise, employees and students who have access to the website of QCS are strictly prohibited from altering the website in any way that will portray QCS in a bad light or reflect poorly upon this school as a Christian educational institution.

The Internet should not be used for personal gain or advancement of individual views, through the use of the QCS network. Likewise, solicitation of non-school business or any use of the Internet for personal gain is strictly prohibited through access to the QCS network. Use of the Internet must not disrupt the operation of the school's network or the networks of other users. Use of the Internet must not interfere with employee or student productivity during the course of regularly scheduled work hours. Employees are required to have their computers protected with sign-on passwords and are encouraged to utilize an automatic screen saver with password protection. Students are strongly encouraged to use sign-on passwords and screen savers. Employees and students are expected to keep passwords and other digital security credentials confidential. Use of another person's identity to access technology and network resources is prohibited.



Each Quakertown Christian School employee and student is responsible for the content of all text, audio, or images that he/she places or sends over the Internet and/or on the school's website. Fraudulent, harassing, or obscene messages, pictures, or other text are strictly prohibited. All messages communicated on the Internet should have the responsible employee's or student's name attached. No messages should be transmitted under an assumed name. QCS Internet users may not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others. Abusive, profane, or offensive language is not to be transmitted through the system. Employees who wish to express personal opinions on the Internet are encouraged to obtain their own usernames on other Internet systems. Users shall not intentionally seek information on other users, modify or obtain copies of files, other data, or passwords belonging to other users, or misrepresent other users on the network. The network will not be used to disrupt the work of others. Hardware or software shall not be destroyed, modified or abused in any way. Employees and students will be responsible for damages to equipment, systems and software resulting from deliberate or willful acts.

System users are liable for any action or negligence that directly or indirectly results in adverse effects upon the system or its users. To prevent computer viruses from being transmitted through the QCS computer system, caution should be used when downloading any files. To this end the following guidelines should be followed by employees and students alike.

QCS protects all school-owned computers with virus protection. Employees must not attempt to disable or otherwise modify the software. QCS strongly encourages cyber-school computers and student-owned computers also be protected by antivirus software that is updated on a regular basis. The Administration of QCS can verify same. Make sure that your files are backed up regularly if you are storing files on your local C: drive. Do not open any files attached to an e-mail from an unknown, suspicious, or untrustworthy source. Do not open any files attached to an e-mail unless you know what it is, even if it appears to come from a friend or someone you know. Exercise caution when downloading files from the Internet. Always ensure the source is legitimate and reputable. Contact the Administration of QCS (employees) or staff member (students) if you are not sure of the source or reliability of the website.

In addition, all Quakertown Christian School employees and students are prohibited from bringing in outside software or files to visit, view, download, transfer or otherwise use pornographic, sexually explicit, obscene or inappropriate material.

All messages created, sent or retrieved over the Internet through the QCS network are the property of QCS and should not be considered private property. QCS reserves the right to access and monitor all messages and files on its computer system as well as all Internet usage as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or receiver.

Any employee who discovers a violation of this policy should immediately notify the Head of School. Any student who discovers a violation of this policy should immediately notify a staff member. Retaliation in any form against a QCS employee or student who exercises, in good



faith, the right to report said violation is strictly prohibited and will itself constitute a basis for appropriate disciplinary action.

If necessary, an evaluation and investigation will be conducted by the Head of School and/or Board. This will be conducted in a thorough, prompt, impartial, and confidential manner as is reasonably possible under the circumstances. The Head of School and/or Board will take the appropriate corrective action when warranted. Any employee who violates any provision of this Internet policy, as set forth above, will be subject to disciplinary action, up to and including unpaid suspension from work or termination of employment. Any student who violates any provision of this Internet policy applicable to students will be subject to disciplinary action. For both employees and students, if necessary and warranted, QCS will advise the appropriate legal authorities.

By accessing the Internet at QCS, an employee or student agrees to be bound by this policy and to comply with all applicable local, state and federal laws and regulations.

Internet Safety Policy

It is the policy of Quakertown Christian School (QCS) to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA")(Pub. L. No. 106-554 and 47 U.S.C. §254(h)).

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter the Internet, World Wide Web, other forms of electronic communications, and access to inappropriate information. Filtering is required for all Internet-enabled computers whether used by minors or adults. Specifically, as required by the Children's Internet Protection Act, the blocking shall be applied to visual depictions of material deemed obscene, to child pornography, to any material deemed harmful to minors, and to any other content deemed inappropriate for minors by local standards. It is acceptable to set different levels of filtering for minors on an age-determinant or individual basis. Technology protection measures may be temporarily disabled by the Director of Information Technology for adults for bona fide research or for other lawful purposes. Even with these safeguards in place, Quakertown Christian School cannot guarantee that a student or staff member will not gain access to objectionable or inappropriate material on the Internet.

To the extent practical, steps shall be taken to promote the safety and security of users of the QCS online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Measures designed to restrict minors' access to materials harmful to minors must be used. Such measures may include: network firewalls, confidential passwords, data encryption, electronic monitoring and physical data security. Inappropriate network usage is prohibited. Inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; (b) unauthorized disclosure, use and dissemination of personal identification information



regarding minors; and (c) illegal sharing/copying of copyrighted works in the form of music, videos, photocopies, photographs, software, performance, audiovisual, multimedia, DVD/CD-ROM, or Laserdisc. However, Facebook and MySpace are not considered inappropriate network usage and are not required to be blocked.

It shall be the responsibility of all Quakertown Christian School staff to educate, supervise and monitor appropriate usage by all minors of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Information Technology or designated representatives.

The classroom teachers or designated representatives will provide annual, age-appropriate training for students who use the QCS online computer network and Internet access. The training provided will be designed to promote the school's commitment to: the standards and acceptable use of Internet services as set forth in the school's Acceptable Use of Internet and Network Resources Policy and Internet Safety Policy; student safety on the Internet, appropriate behavior while online, on social networking Web sites, and in chat rooms, and cyber-bullying awareness and response; online privacy and security issues; and compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training the student's name and date will be recorded in a log book and/or the student will acknowledge that he/she received the training, understood it, and will follow the provisions of Quakertown Christian School's Acceptable Use of Internet and Network Resources policy and Internet Safety Policy.

As defined in the Children's Internet Protection Act ("CIPA") these words have the following meanings.

Minor. The term "minor" means any individual who has not attained the age of 17 years.

Technology Protection Measure. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

- (1) obscene, as that term is defined in 18 U.S.C. §1460;
- (2) child pornography, as that term is defined in 18 U.S.C. §2256; or
- (3) harmful to minors.

Harmful to minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

- (1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
 - (2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulate sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 - (3) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- Sexual act; Sexual contact. The terms "sexual act" and "sexual contact" have the meanings given such terms in 18 U.S.C. §2246.



Approved, October 2013
Revised, August 2019
Reviewed, February 2023