Quincy Public Schools Administrative Procedure

ACCEPTABLE USE PROCEDURE (AUP):

AUTHORIZATION FOR ELECTRONIC NETWORK ACCESS AND COMPUTER USAGE

'Electronic Network(s)' or 'Network(s)' is defined as the District's network (including the wireless network), servers, computer workstations, mobile technologies, peripherals, applications, databases, online resources, Internet access, email, digital accounts, and any other technology designated for use by students and staff, including all new technologies as they become available.

All use of Electronic Networks, including the Internet, shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These rules do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of the *Authorization for Electronic Network Access and Computer Usage* will result in the loss of privileges, disciplinary action, and/or appropriate legal action.** The signature(s) at the end of this document indicates the party who signed has read the terms and conditions carefully and understands their significance.

Terms and Conditions

1. Acceptable Use - Access to the District's network and Internet must be for the purpose of education or research and be consistent with the educational objectives of the District.
2. Privileges - The use of the District's network and Internet is a privilege, not a right, and inappropriate use will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The Superintendent (or his/her designee) will make all decisions regarding whether or not a user has violated these rules and will make the appropriate recommendations. **Students and staff should have no expectations of privacy regarding use of the network. Intrinsic to network administration, system administrators have access to all information associated with electronic communication.**
3. Unacceptable Use – Users are responsible for their actions and activities involving the network. Some examples of unacceptable uses include but are not limited to the following:
   a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
   b. Unauthorized uploading or downloading of software, regardless of whether it is copyrighted or devirused;
   c. Downloading copyrighted material for other than personal use;
   d. Using the computer system for private financial or commercial gain (this includes buying or selling on the Web);
   e. Wastefully using resources, such as file space, personal multimedia, chain letters, flaming, etc.
   f. Gaining unauthorized access to resources or entities;
   g. Trespassing in others' folders, work, files or changing computer files not belonging to the user;
   h. Invading the privacy of individuals;
   i. Using another user's account or password or sharing passwords with others;
   j. Posting material authored or created by another without his/her consent;
   k. Posting anonymous messages;
   l. Using the network for commercial or private advertising;
   m. **Accessing, submitting, posting, publishing or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening (including weapons & bombs), racially offensive, harassing, or illegal messages, pictures, or other material;**
   n. Using the network or Internet while access privileges are suspended or revoked;
   o. Using chat rooms and/or social networking sites without permission.
4. Network Etiquette - Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
   a. Being polite. Not becoming abusive in messages to others.
   b. Using appropriate language. Not swearing, or using vulgarities or any other inappropriate language.
   c. **Not revealing ANY personal addresses or telephone numbers.**
   d. Recognizing that electronic mail (E-mail) is not private. Administrators of the system have access to all mail, files and activity logs. Messages relating to or in support of illegal activities must be reported to the authorities.
   e. Not using the network in any way that would disrupt its use by other users.
   f. Considering all communications and information of others accessible via the network to be private property.
5. Instructional Resources - Users may be granted access to online instructional resources to create a collaborative online environment. The purpose of this access is to create an online environment where users can display and share what they have created. Users will have the opportunity to create websites, multimedia posters, podcasts (audio recording), and videos utilizing educational resources, including but not limited to, learning platforms, blogs, wikis, and podcasts. Users understand that their work may be viewed by others as a public digital format; therefore, users will not reveal personal information. Participation in these resources may require individual digital accounts. Student accounts will be controlled by the district staff.
6. Bring Your Own Device - It is our goal that students and teachers will collaborate in rich, engaging learning experiences using technology. Students may bring their own technology and utilize personal electronic communication devices at school and at school activities. Students may use these devices in the classroom when the teacher deems them appropriate for educational purposes. All devices must remain silent or be put away unless being used within a lesson during class time. Devices should be clearly labeled with student's full name. Students are responsible for personal property brought to school and should keep personal items with self or in a locked space. Devices should be charged prior to bringing them to school. In the event the technology is used inappropriately, disciplinary consequences may occur. The purpose of the District's BYOD program is to extend and enrich the learning environment. The following guidelines apply to students who participate in the program:
   a. Access only the District's Internet gateway. The District filters access to materials that may be defamatory, inaccurate, offensive, or otherwise inappropriate at school pursuant to policy 6:235, Access to Electronic Networks. Make no attempts to bypass the District's Internet gateway. Similar to when a filter is disabled or malfunctions, it is impossible to

control all Internet material, and a BYOD participant may discover inappropriate material. It may also be discovered if and/or when sharing a BYOD device with another student. Report inappropriate content and conduct to your classroom teacher.

b. Follow the standards of your parent/guardians. The District respects each family's right to decide whether or not to participate. District-provided technology may be an alternative.

c. Access only authorized data or files on the computer or Internet sites that are relevant to the classroom curriculum and suggested by a teacher. Students are strictly prohibited from infecting the District's network(s) with a virus or malware program designed to damage, alter, or destroy the network, and hacking, altering, or bypassing security policies. Using anti-virus and anti-malware software on BYOD devices is encouraged. The District may examine any BYOD device that it suspects is causing network problems or may be the source of an attack or virus infection.

d. Use of a BYOD device is subject to policy 7:190, Student Discipline. That means BYOD devices are for curriculum-based instruction only. Students must follow any additional guidelines a classroom teacher or the school might impose. The use of BYOD devices may in no way disturb the learning environment. Students are not allowed to use BYOD devices during test administration. When permitted by school rules, students may use BYOD devices before and after school, during lunch break, during after-school activities, and at school-related functions. BYOD devices may be used while riding to and from school on a school bus or on a school-sponsored activity, at the discretion of the bus driver, classroom teacher, or sponsor/advisor/coach.

e. Transmit only appropriate content while using the District's electronic network. Students may not use BYOD devices to record, transmit, or post photos or audio/video recordings of any person on school property or school-sponsored events without express permission of a teacher or administrator. Any reasonable suspicion of an activity that violates law or Board policies will be treated according to policy 7:140, Search and Seizure. Bullying or sexual material will not be tolerated and will be managed pursuant to policy 7:180, Preventing Bullying, Intimidation, and Harassment. Retrieval of devices that become involved in a law enforcement investigation is the student and parent/guardian's responsibility.

f. Charge all BYOD devices prior to school every day.

g. Turn off and keep BYOD devices in the sight of the teacher during assessments, unless otherwise directed by a teacher. Immediately follow any teacher's instruction to shut down BYOD devices or close the screen. All BYOD devices must be in the silent mode and put away when directed by teachers.

h. Sharing BYOD devices with other students is not a requirement for participation in the BYOD program. From time to time, an assignment may have a collaborative component in which students work together in partners or small groups. In this learning situation, students maintain individual control over their device.

7. No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered by the user. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or user errors or omissions**. Students and staff are responsible for backup of their personal files.** The District specifically denies any responsibility for the accuracy or quality of information obtained via the Internet.
8. Indemnification - To the extent permitted by law, the user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of these rules.
9. Security - Network security is a high priority. If the user can identify a security problem on the network or on the Internet, he/she must notify the system administrator, the building technology facilitator or building principal. The problem should not be described or demonstrated to other users. **Accounts and passwords should be kept confidential. Users should not use another individual's account.** Attempts to log-on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.
10. Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy hardware or data of another user, the Internet, or any computer system. This includes, but is not limited to, the uploading or creating of computer viruses and any attempts to disrupt network resources or communication.
11. Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
12. **These rules may be amended from time to time by posting amendments in the main office of the school. Amendments become binding upon posting. No further signature is required.**

Students and employees need only sign this *Authorization for Electronic Network Access and Computer Usage* once while enrolled or employed by the School District.

Agreement to *Authorization for Electronic Network Access and Computer Usage:*

I understand and will abide by the above ***Authorization for Electronic Network Access and Computer Usage***. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's network and Internet connection and having access to public networks, I hereby release to the extent permitted by law the School District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use the network or the Internet.

DATE: _____, 20____

_____
USER NUMBER (student id / employee number)

_____
USER NAME (please print)

_____
SCHOOL / BUILDING

_____
USER SIGNATURE

PARENTAL CONSENT FOR STUDENTS

Please assist your child to read and comprehend the Quincy Public Schools Authorization for Electronic Network Access and Computer Usage. The purpose of the Authorization for Electronic Network Access and Computer Usage is to provide information on responsible use of technology.

Signing below indicates that I have read the Quincy Public Schools' Authorization for Electronic Network Access and Computer Usage and I understand the policies outlined in the document. Quincy Public Schools has my permission to allow my child to access the Quincy Public Schools networks and access technology for educational purposes, including the Internet. I authorize my student to participate in collaborative online environments that require individual digital accounts. I give permission for sharing of my student's works and performances on/with educational resources, including but not limited to learning platforms, blogs, wikis, and podcasts. I understand that there will be no identifying information (last names) posted. Work may be used by the teacher for future reference as examples of student work. I grant permission to the teacher to create an account for free educational related websites for students under 13 years of age. I have read and explained the Quincy Public Schools Acceptable Use Policy to my child.

I hereby release to the extent permitted by law the School District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use the network or the Internet. In addition, I will accept full responsibility and liability for the results of my child's actions with regard to the use of this technology. I release Quincy Public Schools and any related organizations from any liability relating to consequences resulting from my child's use of the technology.

DATE: _____, 20____

_____
PARENT/GUARDIAN NAME (please print)

_____
PARENT/GUARDIAN SIGNATURE