CANTON PUBLIC SCHOOLS

4 Market Street, Suite 100
Canton, Connecticut 06019
Phone: 860-693-7704 • Fax: 860-693-7706

Opening Minds ~ Transforming Lives

July 1, 2024

Dear Staff:

The Canton Public Schools requires *all* staff to sign the "Regulations for Acceptable Use of Technology," a RAUT, in order to use the district's computers/tablets. The Technology Users' Agreement found on the reverse side of this letter is part of the regulations which follow it.

The form must be returned to the school by September 13, 2024, for you to use the computers and Internet. The full set of Acceptable Use Regulations is also on both the school's and District's websites.

We have set your accounts to expire on September 13, 2024, unless we have a signed RAUT; so kindly help us with this time sensitive paperwork.

Please feel free to contact your school principal if you have any questions or concerns.

Respectfully,

Jon M. Bishop
Assistant Superintendent

Jeffrey R. DelMastro
Information Technology Administrator

Our Mission

Our mission is to prepare independent, productive, respectful and responsible citizens who contribute to an ever changing world. We pursue continuous improvement while honoring our strong education legacy and traditions. We unite with families and the community to provide challenging educational experiences that promote the intellectual, physical, social and emotional potential of our students.

2024-2025 Staff Technology User Agreement

- Staff must sign the acceptable use form below by September 13, 2024, or the account will be closed.

I, _____ (typed or printed name), understand and will abide by the Canton Board of Education's "Regulations for the Acceptable Use of Technology." I further understand that any violation may result in the loss of access privileges and school disciplinary action.

Employee Signature: _____

Date: _____

Food or Drink will not be taken or consumed in computer classrooms or near any workstation.

Canton Public Schools

Certified – Non-Certified Staff

Regulations for Acceptable Use of Technology

Revised July 2024

Reasons for these Regulations:
Canton Board of Education ("CBOE") is providing a computer network and Internet access for its students and teachers. This service allows teachers and students to share information, learn new concepts, research diverse subjects, and create and maintain school-based websites.

CBOE has adopted these "Regulations for Acceptable Use of Technology" (RAUT) to set guidelines for accessing the CBOE Computer Network and/or the Internet service provided by CBOE. Every year, students who want computer network and Internet access for that upcoming school year need to sign and return these "Regulations for Acceptable Use of Technology" to the school within the first two weeks of school in order to maintain their access to technology. In addition, students must have their parents or guardians sign this RAUT. By signing this agreement, the student and parent or guardian agree to follow the rules set forth in this RAUT and to report any misuse of the computer/tablet, the CBOE Computer Network, and/or the Internet to a teacher or supervisor. Parties agreeing to this policy also understand CBOE may revise the Internet Acceptable Use Policy as it deems necessary.

CBOE will provide notice of any changes either by posting a revised version of the RAUT on its website or by providing written notice to the students, employees, and parents or guardians. To obtain access to the CBOE Computer Network and the Internet, students must also follow any school procedures developed at the school site. Each student who qualifies may access the CBOE Computer Network or Internet. The student is required to change the password when prompted and routinely thereafter. The account may only be used during the time the user is a student of the CBOE. Anyone who receives an account is responsible for making sure it is used properly and the password is never given to anyone outside of the Information Technology Staff. Nor should the password be written down and posted to a wall near the computer, taped under the keyboard, or in any way made easy for another person to uncover. The IT staff will *only*

request a user password if a staff member's or student's account requires service, and, as a courtesy, the IT staff can avoid resetting that account to a default password state.

Acceptable Uses of the CBOE Computer Network or the Internet

- The account provided by CBOE should be used only for educational purposes.
- If a user is uncertain about whether a particular use of the CBOE Computer Network or the Internet is appropriate, he or she should consult a teacher or supervisor.

Unacceptable Uses of the CBOE Computer Network or the Internet

The following uses of the account provided by CBOE are unacceptable:

Uses that violate any state or federal law or municipal ordinance are unacceptable.

- *Unacceptable uses of the CBOE Computer Network including Public WiFi include, but are not limited to the following:*
    - Selling or purchasing any illegal substance;
    - Accessing, transmitting, or downloading pornography, obscene depictions, harmful materials, or materials that encourage others to violate the law;
    - Transmitting or downloading confidential information or copyrighted materials;
    - Uses that involve the accessing, transmitting, or downloading of inappropriate matters on the Internet, as determined by the school board, local educational agency, or other related authority;
    - Uses that involve obtaining and/or using anonymous email, proxy sites, VPN sites, or intentionally taking steps to circumvent schools internet filtering.

Uses that cause harm to others or damage to property are unacceptable.

- *Unacceptable uses of the CBOE Computer Network include, but are not limited to the following:*
    - Deleting, copying, modifying, or forging other users' emails, files, or data;
    - Accessing other users' email without their permission, and as a result of that access, reading or forwarding the other user's emails or files;
    - Damaging computer equipment, **putting stickers on computers**, files, data, or the CBOE Computer Network;
    - Using profane, abusive, or impolite language online;
    - Disguising one's identity, impersonating other users, or sending anonymous email messages;
    - Threatening, harassing, or making defamatory or false statements about others;
    - Accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
    - Accessing, transmitting, or downloading computer malware (virus, spyware, etc.) or other harmful files or programs, or in any way degrading or disrupting any computer system performance, including games or chat software.
    - Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes";

- Using any CBOE computer to pursue "hacking," internal or external to CBOE, or attempting to access information that is protected by privacy laws.

Uses that jeopardize access or lead to unauthorized access into Accounts or other computer networks are unacceptable.

- *Unacceptable uses of the CBOE Computer Network include, but are not limited to the following:*
  - Using other users' account passwords or identifiers;
  - Disclosing one's account password to other users or allowing other users to use one's account;
  - writing down the password and posting to a wall near the computer, or taping the password under the keyboard, or in any way making it easy for another person to uncover the password;
  - Getting unauthorized access into other users' accounts or other computer networks;
  - Interfering with other users' ability to access their accounts.
  - Taking any remote control of another computer system, unless established by the IT Staff.

Commercial use Guidelines:

Purchases over the Internet for a project, such as wood class, are permissible *only* with teachers' and/or parents' permission.

- *Unacceptable uses of the CBOE Computer Network include, but are not limited to the following:*
  - Selling or buying anything over the Internet for personal financial gain;
  - Using the Internet for advertising, promotion, or financial gain;
  - Conducting for-profit business activities.

Internet Safety Guidelines for Your Students:

- CBOE will implement filtering and/or blocking software to restrict access to Internet sites containing pornography, obscene depictions, or other harmful materials. The software will work by scanning for objectionable words or concepts, as determined by CBOE and Connecticut Educators Network (CEN). *However, no software is foolproof*, and there is still a risk an Internet user may be exposed to a site containing such materials. A user who incidentally connects to such a site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.
- Students shall not reveal on the Internet personal information about themselves or about other persons. For example, students should not reveal their full names, home addresses, telephone numbers, school addresses, or parents' names on the Internet. An exception to this would be online applications to colleges or job studies or as directed by a teacher. These activities must be pre-approved by a school counselor. Final responsibility for putting personal information on the Internet rests with the individual. Not only on the CBOE Computer Network, but anywhere, it is strongly

recommended that users go to great lengths to determine legitimacy of any online organization.
- Students shall not meet in person in a secluded place or a private setting with anyone they have met on the Internet.
- Students shall not meet in person *in any place with anyone* they have met on the Internet without their parent's permission. CBOE will not endorse any type of meeting with persons students have met on the Internet *without* pre-approval in writing.
- Account users will abide by all school security policies.

Privacy Policy:

- The School District Administration has the authority to monitor, inspect, copy, review, and store at any time and without prior notice all accounts, including email and any information transmitted, received, and/or created on any computer or user account. All such materials are the property of CBOE.
- The Superintendent or his designees will periodically conduct searches to see if teachers have posted inappropriate materials on-line. When inappropriate use of computers or websites is discovered, the School Principals and Superintendent will download the offensive material and determine the appropriate disciplinary action. (from Board of Education Policy 4118.51 (b) / 4218.51.)
- Account users do not have any right to, or expectation of, privacy regarding such materials.
- Please be aware that Canton monitors all internet activity including but not limited to email and web access. This can include review of emails sent and received for up to five years. In addition all internet sites are recorded by user account and automated reports are generated based on inappropriate use.
- All such information files created or accessed on any Canton owned computer may be recorded and reviewed.
- Real time monitoring of all computer systems when in use can include remotely watching the screen or taking over the workstation. This monitoring is generally used to provide technical support to the user from a remote site.
- Offensive or inappropriate material gained in any of the above means will be submitted to an appropriate supervisor or legal representatives for disciplinary recommendations.
- Use of Google Education Suite is heavily used in Canton Public Schools, and by signing this agreement you authorize the use of Google services including, but limited to Maps, Gmail, YouTube, Classroom, etc. where deemed appropriate by school administration.
- Computers, tablets, and all electronic services owned or licensed by CBOE are the property of CBOE. Any and all documents created on these devices are the sole ownership of the CBOE and may be seized or reviewed without notice. These devices are not for your personal use.

E-mail & Cloud services use:

- At this time, student use of personal email is permitted, but this is subject to change as state and federal guidelines mandate. Local school policy may be more restrictive and should be consulted prior to beginning use of these services.
- If a user is accessing personal email through the CBOE Computer Network, it should be for the purpose of education only. E-mails using personal email accounts are discouraged. Please encourage your students to email using school accounts rather than personal email accounts.
- CBOE does *not* permit transferring programs or apps via email or cloud based storage services such as google cloud.
- CBOE explicitly prohibits the sharing of 'sensitive' data through any method whatsoever without explicit administrative approval.
- CBOE explicitly prohibits the streaming of video or audio without administrative approval.

Games:

- Only approved educational games under the direct supervision of a teacher in whole-class instruction will be allowed.
- Staff should use their best judgment on how gaming can be best used in an instructional setting.

The Board has developed a Social Networking Policy 4118.51 (a) / 4218.5 for all Certified and Non-Certified Personnel. It is each individual's responsibility to become familiar with this policy, which is linked here. Failure to adhere to the Board policy may lead to dismissal if the employee has behaved in any unethical or lascivious way, or if there is a reasonable and adverse relationship between the conduct and the continuing ability of the employee to perform any of his/her professional functions in an effective manner.
What follows are the regulations which support this policy and apply to the use of district computers.

Social Networking Guidelines:

All district employees are expected to behave honorably in on-line activities. Activities which are improper, unethical, and illegal or which cause undue discomfort for students, employees, parents, or other members of the school community should be avoided in both physical space and cyberspace. To that end, the following regulations for school employees who use networking applications, such as, but not limited to Facebook, LinkedIn, Twitter, etc., which may be frequented by current or former students are provided. These guidelines apply to employees' personal use of social media from their own computers and devices as well. Again, reference the Board policy above.

- Do not accept or initiate students as friends on personal social networking sites. Decline student-initiated and parent-initiated friend requests.
- Do not access social networking sites for personal use during school hours.
- Do not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks, or characterizations.

- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- Do not discuss students or co-workers or publicly criticize school policies or personnel.
- If you learn information through a social networking site that falls under the mandatory reporting guidelines, report it as required by law.
- Visit your profile's security and privacy settings. Staff members should have all privacy settings set to "Only Friends."
- Remind all members of your network that, due to your position as a school system employee whose profile may be accessed by current or former students, they should monitor their posts to your network accordingly. Conversely, be judicious in your postings to your friends' sites. Act immediately to remove from your site any material that may be inappropriate whether posted by you or someone else.
- Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these applications include calendars and games.
- Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
- If a staff member is going to use social media they should provide their administrator with written information on how to view what is in the feed (i.e., Twitter handle, any #'s being used).

AI, Chat Rooms, Blogs, Discussion Boards:

- Access to chat rooms, blogs, and discussion boards is restricted to educational use only.

- Artificial Intelligence (AI) services will be restricted to approved solutions only. We do realize this platform is changing quickly and even search engines now provide AI assistance. As the data model that these services utilize have not been vetted, you should consider the results suspect. For more information, please refer to the district's AI guidance guidelines.

Personal Computers/Devices (BYOD):

- The Board of Education is committed to aiding students and staff in creating a 21st century learning environment. Therefore, students and staff will be permitted to access the District's "Public" wireless network with their personal devices during the school day. The internet shall be made available to students for instructional purposes in accordance with administrative regulations.
- The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his/her electronic device while at school. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole.
- Students and parents/guardians participating in the Bring Your Own Device program must adhere to the Student Code of Conduct, as well as all applicable Board policies, particularly the Computer Acceptable Use policy.
- The use of these devices, as with any personally owned device, is strictly up to the teacher.

- Each student/parent guardian will be required to sign the BYOD User Agreement Form.
- The public WiFi network may be shut down, filtered, and limited at any time by the Information Technology department.

User name and passwords:

- User must have a signed user agreement on file within 10 business days of the start of school or those services will be suspended.

Passwords:

User names and initial passwords will be assigned. Generally this is in the form of the first initial last name, but Information Technology reserves the right to assign any name based on what is available.

- Passwords will be a minimum of 6 characters long and a maximum of 8 characters long.
- As a guideline, passwords should be a combination of numbers, characters, and punctuation characters and should not be something personal.
- For staff and contractors, some services now require Multi Factor Authentication (MFA or 2FA) for the purposes of keeping your information secure.

Penalties for Improper Use:

All computers, tablets, and Chromebooks have remote monitoring software installed on them, enabling IT staff and select administrative personnel to remotely view the work being done on that computer. The use of the CBOE Computer Network and equipment, including the account, is a privilege, not a right.

- Inappropriate use may result in the restriction or cancellation of the account.
- Inappropriate use may lead to any disciplinary and/or **legal** action, including but not limited to suspension or expulsion or criminal prosecution by government authorities.
- CBOE will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

Food or Drink will not be taken or consumed in computer classrooms or near any workstation!