



CANTON PUBLIC SCHOOLS

4 Market Street - Suite 100, Canton, CT 06019-3146
Tel. (860) 693-7704 Fax (860) 693-7706
www.cantonschools.org

Lynn K. McMullin
Assistant Superintendent of Schools
lmcnullin@cantonschools.org

July 25, 2009

Dear Staff,

Canton requires *all* students and staff members to sign an "Acceptable Use Policy," an AUP, in order to use the district's computers. The users' agreement is part of regulations attached to this letter, and it must be returned to the school by September 14th for your continued use of the computers and Internet. The full set of Acceptable Use Regulations, (a much more complex document than included here), is available on District website.

Two years ago, Canton had an SAS94 Audit; and as a result, to certify all District Office data and to meet State requirements, we are required to have all our users sign an AUP. We have spent many thoughtful hours developing this policy. New this year are regulations for teachers/staff members who maintain social networking pages such as *Facebook* or *My Space* (page 6). Please read this section carefully, especially if you socially network. There is also a clearer explanation of the ability of IT staff to remotely monitor the work being done on any computer (page 5).

The students will once again be required to sign an AUP, as well. We have set the students' accounts to expire on September 14, 2009, unless we have a signed AUP from home; so kindly help us with this time sensitive paperwork.

Technology is a tremendous aid to education in our schools and we don't want any interruptions in our programs, so we appreciate your attention to this new regulation.

Sincerely,

Lynn K. McMullin

2009 – 2010 Technology User Agreement:

- Staff members must sign the acceptable use form below by September 14, 2009 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.

Staff Signature: _____

Date: _____

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

The seal of Canton Public Schools is a circular emblem. It features a central figure holding a scale of justice, with a book open below. The words "CANTON PUBLIC SCHOOLS" are written around the perimeter of the seal. The seal is faintly visible in the background of the title page.

Canton Public Schools

Regulations for Acceptable Use of Technology – Staff Copy

Revised July 2009

Reasons for this Policy

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, 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 include, but are not limited to the following:
 - Selling or purchasing any illegal substance;
 - Accessing, transmitting, or downloading child 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 or web proxy sites.

Uses that cause harm to others or damage to their 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' e-mails, files, or data;
 - Accessing other users' email without their permission, and as a result of that access, reading or forwarding the other user's e-mails or files;
 - Damaging computer equipment, 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:

- 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. These activities must be pre-approved by a guidance 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 recommend 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 anyone they have met on the Internet.
- Students shall not meet in person *in any place* anyone they have met on the Internet without their parent's permission. CBOE will not endorse of 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 System Administrator has the authority to monitor all accounts, including e-mail and other materials transmitted, received, and/or created on any computer or user account. All such materials are the property of CBOE.
- Account users do not have any right to, or expectation of, privacy regarding such materials.
- Each account user of the CBOE Computer Network does have the right to know exactly what can be monitored and how. Please be aware that through the user accounts Canton monitors all internet activity including 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 files created or accessed on any Canton owned computer are automatically recorded and can be 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 the any of the above means will be submitted to an appropriate supervisor with disciplinary recommendations.

E-mail 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. As it stands now, student email is *never* allowed to be accessed at CIS or CBPS.
- If a user is accessing personal email through the CBOE Computer Network, it should be for the purpose of education only. This would include transferring documents created by the student to the teacher.
- CBOE does *not* permit transferring programs via email.
- Suggested method for transferring homework is using a USB Flash drive.
- Emailing grades or attendance is *prohibited*.

Games:

- Only approved educational games under the direct supervision of a teacher in whole-class instruction will be allowed.
- Accessing or attempting to access games online is not permitted and is considered in violation of this RAUT.

Social Networking:

- *Facebook, My Space* and other cyber social networking opportunities have changed the potential for relationships. However, the definition of an acceptable teacher/student relationship *before* the digital age is the same definition to be applied in every decision regarding teacher/student relationships in the *new* digital age. In other words, a staff member and a student would not have been friends *before* social

networking and *should not be “friends” now*. The same rules that a staff member would apply to telephoning a student directly, to meeting a student or group of students outside of school, to socializing with students, and so on apply to digital age contexts such as emailing, texting, chat rooms, and all types of social networking’s virtual “meetings.”

- Teachers who engage in social networking, i.e. who maintain personal *My Space* or *Facebook* pages, for example, have an obligation to maintain their pages in an appropriate and responsible way. It is recommended that staff member’s personal pages be maintained with all of the privacy features offered by the host site.
- Under no circumstances shall a staff member extend “friend” privileges to a student or become a friend on a student’s page.
- Teachers *shall not in any way engage in online or digital* student-to-student discussions. This includes chat room gossip, name calling, taunting, petty disputes, sexually-charged discussions, spamming, etc. *even for the purpose of mollifying the discussion*. Teachers may report witnessing such a discussion to the Building Principal and/or his/her designee, but should not act on it alone.
- Teachers and staff members who witness acts of cyber-bullying, extortion, or any online threats to the health and safety of a student or students shall promptly notify the Building Principal and/or his/her designee of the events observed, and shall promptly file a written incident report concerning the events witnessed.

Chat Rooms, Blogs, Discussion Boards:

- Access to chat rooms, blogs, and discussion boards is restricted to educational use only. This will be led by a staff member and must be pre-approved by a building level administrator prior to the lesson.
- No instant messaging will be permitted, unless the teachers and/or students have met with the above qualifications.

Storage Capacity:

- Each student will be allowed up to 200MB of storage. More space may be made available upon request providing it is warranted by a teacher and only if there are no technical problems with the request. Accounts that exceed the disk quota will not be able to save until files are deleted
- To ensure that account users remain within the allocated disk space, students should periodically delete unwanted files or data that are no longer needed and take up excessive storage space.

Personal Computers:

- Personal computers from home are only allowed to be used on CBOE Computer Network *after* they have been verified by a System Administrator. Any utilities used for hacking, peer-to-peer file sharing, or sniffing will be immediately barred from Canton Schools.

- Some schools may not allow student computers on their network. Always check with your building level IT support for site specific rulings.

Prior to receiving a user name and password:

- User must have a signed user agreement on file.

Passwords:

- User names and passwords will be assigned. Generally this is in the form of first initial last name, but the System Administrator 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 and characters and should not be something personal.

Penalties for Improper Use:

- All computers will 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!