

August 22, 2014

Dear Staff Member,

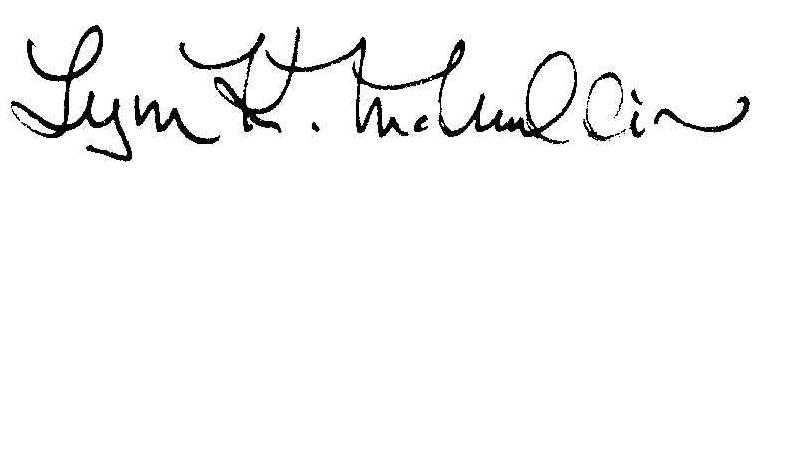
Orange Public Schools requires *all* certified and non-certified staff members to sign the “Regulations for Acceptable Use of Technology,” a RAUT, in order to use the district’s computers. We have applied for, and received, over $15,000 in eRate funding, and a signed RAUT for each staff member is one portion of our audit.

A RAUT protects you as well as protecting the district in our technology-sensitive world. 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 Friday, September 12th for you to use the computers and Internet. The full set of “Regulations for Acceptable Use of Technology” is also available to all staff members on the school web sites and on the Central Office page.

We have spent many thoughtful hours developing this policy. Emphasized this year: a fully developed set of regulations for social networking sites including, but not limited to Facebook, MySpace, You Tube, Twitter, etc. (See pages 7 - 8). *Regulations prohibit teachers/staff members who maintain social networking pages from adding students as friends.* We also added a clearer explanation of the ability of Technology Department staff and administrators to remotely monitor the work being done on any computer (See page 6). This monitoring has always been possible in Orange; but, in the past, the district *did not notify* staff members that it could do so. We have set the accounts to expire on September 12, 2014, unless we have a signed RAUT; so kindly help us with this time sensitive paperwork.

Technology is a tremendous aid to our productivity and educating our students and we don’t want any interruptions in our programs, so we appreciate your attention to this new regulation.

Sincerely,



Lynn K. McMullin

Superintendent

Orange Public Schools

**2014 – 2015**

**Technology User Agreement:**

* Staff members must sign the acceptable use form below by September 12, 2014 or the account will be limited to access to district-wide tools.

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (typed or printed name), understand and will abide by the Orange 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.**

**Orange School District**

**Certified and Non-Certified Staff**

**Regulations for Acceptable Use of Technology – Web Copy**

**Revised August 2014**

**Reasons for these Regulations:**Orange Board of Education (“OBOE”) 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.

OBOE has adopted these “Regulations for Acceptable Use of Technology” (RAUT) to set guidelines for accessing the OBOE Computer Network and/or the Internet service provided by OBOE. 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 OBOE Computer Network, and/or the Internet to a teacher or supervisor. Parties agreeing to this policy also understand OBOE may revise the Internet Acceptable Use Policy as it deems necessary.

OBOE 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 OBOE Computer Network and the Internet, students must also follow any school procedures developed at the school site. Each student who qualifies may access the OBOE 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 OBOE. 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 OBOE Computer Network or the Internet**

* The account provided by OBOE should be used only for educational purposes.
* If a user is uncertain about whether a particular use of the OBOE Computer Network or the Internet is appropriate, he or she should consult a principal or the Technology Administrator, Matthew Bruder.

**Unacceptable Uses of the OBOE Computer Network or the Internet**

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

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

* *Unacceptable uses of the OBOE 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.

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

* *Unacceptable uses of the OBOE 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 OBOE 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 OBOE computer to pursue “hacking,” internal or external to OBOE, or attempting to access information that is protected by privacy laws.

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

* *Unacceptable uses of the OBOE 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 art class, are permissible *only*

with a teachers’ and/or parents’ permission.

* *Unacceptable uses of the OBOE 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:**

* OBOE 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 OBOE 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 OBOE 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. OBOE 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 School District Administration has the authority to monitor, inspect, copy, review, and store at any time and without prior notice all accounts, including e-mail and any all information transmitted, received, and/or created on any computer or user account. All such materials are the property of OBOE.
* The Superintendent or her 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.
* Each account user of the OBOE Computer Network does have the right to know exactly what can be monitored and how. Please be aware that through the user accounts Orange monitors all internet activity including email and web access. This can include review of emails sent and received. 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 Orange 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 OESS.
* If a user is accessing personal email through the OBOE Computer Network, it should be for the purpose of education only. This would include transferring documents created by the student to the teacher.
* OBOE does *not* permit transferring programs via email.
* Suggested method for transferring homework is using a USB Flash drive.

**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.

***INTERNAL* Social Networking:**

* Advise your administrator, fellow teachers, and parents about your internal academic social networking.
* Use the school-supported networking tools.
* Do not say or do anything in the networking environment that you would not say or do as a teacher in the classroom.
* Have a clear statement of purpose and outcomes for the use of the networking tool.
* Establish a code of conduct for students and all network participants.
* Do not post images that include students who are on the school’s ‘do not photograph’ list.
* Pay close attention to the site’s security settings and allow only approved participants access to the site.

***EXTERNAL* Social Networking:**

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, MySpace, 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 or their parents 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.

**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 teacher will be allowed up to 1GB of storage. (Each student is allowed 200 MB 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 OBOE 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 Orange 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, a RAUT contract, 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.
* 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 OBOE 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.
* OBOE 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!**