**EMPLOYEE USE OF THE DISTRICT'S TECHNOLOGY SYSTEMS**

# Litchfield School District
# Certified and Non-Certified Staff
# Regulations for Acceptable Use of Technology
# Revised August 2015

**Reasons for these Regulations:**

Litchfield Board of Education ("LBOE") 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.

These "Regulations for Acceptable Use of Technology" (RAUT) provide guidelines for accessing the LBOE Computer Network and/or the Internet service provided by LBOE. Every year, staff members 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. By signing this agreement, staff agree to follow the rules set forth in this RAUT and understand the Regulations for Acceptable Use of Technology may be revised from year to year as necessary.

The Technology Department will provide notice of any changes by posting a revised version of the RAUT on its website and by providing written notice to the students, employees, and parents or guardians.

To obtain access to the LBOE Computer Network and the Internet, staff must also follow any procedures developed at the school site. Staff is required to change the password when prompted. The account may only be used during the time the user is a staff of the LBOE. 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 the students or another person to uncover. The IT staff will *only* request a user password if a staff member's account requires service and, as a courtesy, the IT staff wants to avoid resetting that account to a default password state.

**Acceptable Uses of the LBOE Computer Network or the Internet**

- The account provided by LBOE should be used only for educational purposes.
- If a user is uncertain about whether a particular use of the LBOE Computer Network or the Internet is appropriate, he or she should consult a principal or the Technology Coordinator, Jamie Terry.

**Unacceptable Uses of the LBOE Computer Network or the Internet**
The following uses of the account provided by LBOE are unacceptable:

1. **Uses that violate any state or federal law or municipal ordinance are unacceptable.**
   - *Unacceptable uses of the LBOE 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
     - Uses that involve obtaining and/or using anonymous email or web proxy sites.

2. **Uses that cause harm to others or damage to their property are unacceptable.**
   - *Unacceptable uses of the LBOE 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 LBOE 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 LBOE computer to pursue "hacking," internal or external to LBOE, or attempting to access information that is protected by privacy laws.

3. **Uses that jeopardize access or lead to unauthorized access into Accounts or other computer networks are unacceptable.**
   - *Unacceptable uses of the LBOE 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 for staff *within the district's guidelines*. If uncertain, call the school office or Central Business Office

*Unacceptable uses of the LBOE Computer Network include, but are not limited to the following:*

- Student purchases, even for a project, over the Internet *without* their parent's permission;
- 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:**

- LBOE and the IT Department 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 LBOE 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. If a user sees another user accessing inappropriate sites, he or she should notify a supervisor immediately.
- Staff should know that 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 LBOE Computer Network, but anywhere, it is strongly recommend that users go to great lengths to determine legitimacy of any online organization.

- Staff should know that students shall not meet in person in a secluded place or a private setting anyone they have met on the Internet. Knowledge of such a meeting should be reported to an administrator.
- Staff should know that students shall not meet in person *in any place* anyone (including pen-pals, project mentors, authors, etc.) they have met on the Internet without their parent's permission. LBOE 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 email and any all information transmitted, received, and/or created on any computer or user account. All such materials are the property of LBOE.
- The Superintendent or designees may 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.
- Account users do not have any right to, or expectation of, privacy regarding such materials.
- Each account user of the LBOE Computer Network does have the right to know exactly what can be monitored and how. Please be aware that through the user accounts Litchfield has the capability to monitor 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 Litchfield 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.
- Staff should know that if a user is accessing personal email through the LBOE Computer Network, it should be for the purpose of education only. This would include transferring documents created by the student to the teacher.
- LBOE does *not* permit transferring programs via email.

**Games:**

- Only approved educational games under the direct supervision of a teacher in whole-class or small-group 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:**

- 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 4118.51 – 4218.51.

- Because teachers and students are not friends, do not accept or initiate students as friends on personal social networking sites. Decline student-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.
- Make sure that expressed opinions are yours alone and that you are not speaking on behalf of your colleagues or District.
- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- Do not post pictures of students or coworkers without their permission.
- Do not discuss students or co-workers or publicly criticize school policies or personnel.
- Do not post District logos or images, or use your district email address.

- 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 type of activity 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:**

- To ensure that account users remain within the allocated disk space, students and staff should periodically delete unwanted files, data, and images that are no longer needed and take up excessive storage space.

**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 last name first initial, 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 LBOE 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.
- LBOE will attempt to tailor any disciplinary action to meet the specific concerns related to each violation.

**Food or drink should not be taken or consumed in computer classrooms or near any workstation. Portable devices should be protected from temperature extremes and should not be left in cars or in direct sun for long periods of time.**