LEBANON COUNTY CAREER AND TECHNOLOGY CENTER

No. 340

Section: ADMINISTRATIVE EMPLOYEES

Title: ACCEPTABLE USE OF INTERNET AND COMPUTERS

Adopted: April 17, 2001

Revised: June 16, 2009, May 18, 2010

340. ACCEPTABLE USE OF INTERNET AND COMPUTERS

1. Purpose

The Joint Operating Committee supports use of the Internet and other computer networks in the Lebanon County Career and Technology Center's instructional program in order to facilitate learning and teaching through interpersonal communications and access to information, research, and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the Joint Operating Committee as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

A form will be signed by each authorized user annually to document:

1. The receipt of the policy by the authorized user.
2. The authorized users acknowledgement to be responsible for all portions of the Acceptable Use of Internet and Computers Policy and any consequences arising from violations of the Acceptable Use of Internet and Computers Policy.
3. These signed forms will be kept on file for a period of not less than three years.

2. Definitions

Authorized User – Those persons who have completed and signed the Internet & Computer Use Agreement Form and have been granted access by the Network Administrator.

Vandalism – Any act that destroys or damages the computer, associated components and cables, as well as programs, data files, and intellectual property not legally owned by the vandal.

3. Authority

The electronic information available to students and staff does not imply endorsement of the content by the LCCTC, nor does the LCCTC guarantee the accuracy of information received on the Internet. The LCCTC shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.

The LCCTC shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The LCCTC reserves the right to log network use and to monitor fileserver space utilization by users, while respecting the privacy rights of both LCCTC authorized users and outside users. No expectation of privacy for any user should be implied or assumed.

The Joint Operating Committee establishes that the use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

The JOC shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.

4. Delegation of Responsibility

The LCCTC shall make every effort to ensure that this educational resource is used responsibly by authorized users.

Administrators, teachers, and other staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other authorized used in the LCCTC and on the Internet.

The Building Administrator shall have the authority to determine what inappropriate use is.

The Administrative Director or designee shall be responsible for recommending technology and developing procedures used to determine whether the LCCTC's computers are being used for purposes prohibited by law or for accessing sexually explicit materials, or for accessing other material deemed inappropriate for an authorized user. The procedures shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for authorized users to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by authorized users by the JOC.
2. Maintaining and securing a usage log.
3. Monitoring all activities of authorized users.

5. Guidelines

Network accounts shall be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be school property and shall not be disclosed without administrative approval. Authorized users shall respect the privacy of other users on the system.

<u>Prohibition and Responsibilities</u>

Authorized users are expected to act in a responsible, ethical, and legal manner in accordance with JOC policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Authorized users may not use a computer or components that will facilitate illegal activity.
2. Authorized users may not use the computer or components for commercial or for-profit purposes.
3. Authorized users may not use the computer or components for non-work or non-school related activities.
4. Authorized users may not use the computer or components for creating product advertisement or political lobbying.
5. Authorized users may not use the computer or components for Bullying/Cyberbullying purposes.
6. Authorized users may not use the computer or components for hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Authorized users may not use the computer or components to gain access to obscene, semi-pornographic (partially disrobed), or pornographic material or child pornography.
8. Authorized users may not use the computer or components to access material that is harmful to minors or is determined inappropriate for minors in accordance with JOC policy.
9. Authorized users may not use the computer or components for the transmission of material likely to be offensive or objectionable to recipient(s) such as, but not limited to profanity, sexual or racial innuendo, drug or drug paraphernalia, etc.
10. Authorized users may not use the computer or components for intentionally obtaining or modifying of files, passwords, and data belonging to other authorized users.
11. Authorized users may not use the computer or components for the purpose of impersonating another authorized user, anonymity, and pseudonyms.
12. Authorized users may not use the computer or components for the purpose of fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Authorized users may not use the computer or components for loading or using of unauthorized games, program files, or other electronic media.
14. Authorized users may not use the computer or components for the purpose of disrupting the work of others.
15. Authorized users may not use the computer or components for the purpose of relocation, destruction, modification, abuse, or unauthorized access to network hardware, software, wires, connections, and files.
16. Authorized users may not use the computer or components to create a personal communication using quotes in a public forum without the original author's prior consent.
17. Authorized users may not use the computer or components for the development or delivery of programs that harass other authorized users or infiltrate a computer system and/or damage the software components of a computer or system is prohibited.
18. The Electronics Communications Privacy Act places electronic mail in the same category as messages delivered by the U.S. Postal Service. Therefore, Authorized users may not use the computer or components to tamper, interfere, intercept or use electronic mail for criminal purposes.

19. Authorized users may not use the computer or components for accessing, copying, or downloading music, video, or other files from the Internet or other devices to any location on the network or device attached to any school hardware.
20. Authorized users may not use the computer or components for uploading any material from personal devices.
21. Authorized users may not use the computer or components for making any changes to computer settings including, but not limited to, screen savers, desktop screen, etc.
22. Authorized users may not use the computer or components to save data or files of any kind to the desktop.
23. Authorized users may not delete the Internet history, temporary Internet files, or local user files on any computer.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or school files. To protect the integrity of the system, the following guidelines shall be followed:

1. Authorized users shall not reveal their password to another individual.
2. Authorized users are not to use a computer that has been logged in under another authorized user's name.
3. Any authorized user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
4. User passwords shall be changed at the discretion of the Network Administrator. Passwords will include at least one of the following types of characters: lower case letters, uppercase letters, numbers, and special characters. The password will be of a minimum length that will be determined by the Network Administrator.

Consequences For Inappropriate Use

The authorized user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges.

Copyright

The illegal use of copyrighted software by authorized users is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

The use of video, technology materials, computer software, etc. which is protected under the copyright laws, will not be transmitted nor stored without the express written permission of the copyright owner.

Safety

To the greatest extent possible, authorized users of the network will be protected from harassment and unwanted or unsolicited communication. Any authorized user who receives threatening or unwelcome communications immediately shall bring them to the attention of a teacher or administrator. Authorized users shall not reveal personal information to other authorized users on the network, including chat rooms, e-mail, Internet, etc.

Any LCCTC computer/server utilized by authorized users shall be equipped with Internet blocking/filtering software.

Internet safety measures shall effectively address the following:

1. Control of access by authorized users to inappropriate matter on the World Wide Web.
2. Safety and security of authorized users when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by authorized users, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of authorized users' access to material harmful to them.

References

School Code – 24 P.S. Sec. 1303.1-A
Child Internet Protection Act – 24 P.S. 4601 et seq.
Enhancing Education Through Technology Act of 2001 –
20 U.S.C Sec. 6777
Internet Safety – 47 U.S.C. Sec. 254
JOC Policies 813, 234, 340, 443 and 538