815. ACCEPTABLE USE OF THE COMMUNICATIONS AND INFORMATION SYSTEMS

1. Purpose

The Lehigh Career & Technical Institute (LCTI) provides employees, students, and guests (Users) with hardware, software and access to the LCTI’s Electronic Communication Systems and network, which includes Internet access, whether wired or wireless, cellular, cloud or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students Joint Operating Committee (JOC) Board members and LCTI consultants and vendors.

Computers, network, Internet, Electronic Communications, information systems, databases, files, software, and media, collectively called “CIS systems”, provide vast, diverse and unique resources. LCTI will provide access to LCTI’s CIS systems for Users if there is a specific LCTI-related purpose to access information to research to collaborate to facilitate learning and teaching and/or foster the Educational Purpose and mission of LCTI.

For Users, LCTI’s CIS systems must be used for Education-related Purposes and performance of LCTI job duties in compliance with this Policy, other LCTI policies, regulations, rules, procedures, Internet Service Provider (ISP) terms, and local, state, and federal laws. Incidental personal use of LCTI computers is permitted for employees as defined in this Policy. Students may only use the CIS systems for educational purposes.

CIS systems may include LCTI computers which are located or installed on LCTI property, at LCTI events, connected to the LCTI’s network, or when using its mobile computing equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when Users bring and use their own personal Computers or personal electronic devices, and, if relevant, when Users bring and use another entity’s Computer or electronic device to a LCTI location, event or connect it to the LCTI network.
If Users’ bring personal Computers or personal electronic devices onto LCTI property, to LCTI events, or connect them to the LCTI’s network and systems, and if the LCTI reasonably believes the personal Computers and/or personal electronic devices contain LCTI information or contain information that violates an LCTI policy or administrative regulation, the legal rights of the LCTI or another person, or involves significant harm to the LCTI or another person, or involves a criminal activity, the personal Computers or personal electronic devices may be legally accessed in accordance with the law to ensure compliance with this Policy, other LCTI policies, regulations, rules, procedures, ISP terms, and local, state and federal laws. Users may not use their personal Computers and personal technology electronic devices to access the LCTI’s intranet, Internet or any other CIS system unless approved by the Supervisor of Technology, and/or designee.

LCTI intends to strictly protect its CIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these LCTI assets and in lessening the risks that can destroy these important and critical assets. Consequently, users are required to fully comply with this Policy, and to immediately report any violations or suspicious activities to the Supervisor of Technology, and/or designee. Conduct otherwise will result in actions further described in Consequences for Inappropriate, Unauthorized and Illegal Use section, found in the last section of this Policy, and provided in other relevant LCTI policies, regulations, rules and procedures.

2. Definitions

20 U.S.C. § 6777;
18 U.S.C. § 2256(8);
47 U.S.C. § 254(h)(7)(F)

Child Pornography - under federal law, any Visual Depiction, including any photograph, film, video, picture, or Computer or Computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

1. The production of such Visual Depiction involves the use of a Minor engaging in sexually explicit conduct;

2. Such Visual Depiction is a digital image, Computer image, or Computer-generated image that is, or is indistinguishable from, that of a Minor engaging in sexually explicit conduct; or

3. Such Visual Depiction has been created, adapted, or modified to appear that an identifiable Minor is engaging in sexually explicit conduct.
Under *Pennsylvania* law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film videotape, Computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited Sexual Act or in the simulation of such act is guilty of a felony of the third degree for their first offense, or guilty of a felony of the second degree for a second offense.

<table>
<thead>
<tr>
<th>18 Pa. C.S.A. § 6312(d), 24 P.S. § 4603</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer</strong> - includes any LCTI owned, leased or licensed or User-owned personal hardware, software, or other technology used on LCTI premises or at LCTI events, or connected to the LCTI network, containing LCTI programs or LCTI student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. Computer includes, but is not limited to, LCTI and Users’ desktop, notebook, powerbook, tablet PC or laptop computers, servers, firewalls/security systems, distance learning equipment, videoconference units, printers, facsimile machines, cables, modems, and other peripherals; specialized electronic equipment used for students’ special education purposes; radio-frequency identification (RFID) and global positioning system (GPS) equipment; personal digital assistants (PDAs); iPods, MP3 players; USB/jump drives; iPads, Kindles, and other eReaders; iPhones, cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities and configurations, telephones, mobile phones, or wireless devices, two-way radios/telephones and other smartphones; beepers; paging devices; laser pointers and attachments; Pulse Pens, and any other such technology developed.</td>
</tr>
</tbody>
</table>

**Electronic Communications Systems** - any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, an Electronic Communications System means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission/transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, wire or electronic communications and any Computer facilities or related electronic equipment for the electronic storage of such communications.

Examples include, but are not limited, the Internet, intranet, electronic mail services, text messaging, GPS, PDAs, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities and configurations.
<table>
<thead>
<tr>
<th><strong>Educational Purpose</strong> - includes use of the CIS systems for classroom activities, professional or career development, and to support LCTI’s curriculum, policies and mission statement.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Harmful to Minors</strong> - under federal law, any picture, image, graphic image file or other Visual Depictions that:</td>
</tr>
<tr>
<td>1. Taken as a whole, with respect to Minors, appeals to the prurient interest in nudity, sex or excretion;</td>
</tr>
<tr>
<td>2. Depicts, describes, or represents in a patently offensive way with respect to what is suitable for Minors, an actual or simulated Sexual Act or Sexual Content, actual or simulated normal or perverted Sexual Acts, or lewd exhibition of the genitals, and</td>
</tr>
<tr>
<td>3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to Minors.</td>
</tr>
<tr>
<td>Under Pennsylvania law, that quality of any depiction or representation in whatever form, of nudity, Sexual Conduct, sexual excitement, or sadomasochistic abuse, when it:</td>
</tr>
<tr>
<td>1. Predominantly appeals to the prurient, shameful, or morbid interest of Minors; and</td>
</tr>
<tr>
<td>2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and</td>
</tr>
<tr>
<td>3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for Minors.</td>
</tr>
</tbody>
</table>


**18 Pa. C.S.A. § 5903(e)(6); 24 P.S. § 4603**
**Inappropriate Matter** - includes, but is not limited to visual, graphic, video, text and any other form of Obscene, pornographic, sexually explicit, indecent, Child Pornographic, or other material that is Harmful to Minors. Examples include: taking, disseminating, transferring, or sharing, whether by electronic transfer (such as sexting, emailing, texting, among others) or otherwise, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminating (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying/cyberbullying, sexting, flagging, terrorist, and other inappropriate matter and material specified throughout this Policy, and other LCTI policies, regulations, rules and procedures. It also includes advocating the destruction of property.

**Incidental Personal Use** - incidental personal use of school Computers is permitted for employees so long as such use does not interfere with the employee’s job duties and performance, with system operations, or with other systems Users, or is excessive. Personal use must comply with this Policy and all other applicable LCTI policies, regulations, rules, and procedures, as well as ISP terms, local, state and federal laws and must not damage LCTI’s CIS systems.

**Minor** - for purposes of compliance with the federal Children’s Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, Minor shall mean the age of minority as defined in the relevant law.

**Obscene** - under federal law, analysis of the material meets the following elements:

1. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state or federal law to be Obscene; and

3. Whether the work taken as a whole lacks serious literary, artistic, political, educational or scientific value.
Under Pennsylvania law, analysis of the material meets the following elements:

1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

2. The subject matter depicts or describes, in a patently offensive way, Sexual Conduct described in the law to be Obscene; and

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Sexual Act and Sexual Contact - as defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3), and 18 Pa. C.S.A. § 5903.

Technology Protection Measure(s) - a specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornography or Harmful to Minors.

Visual Depictions - undeveloped film and videotape and data stored on Computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format, but does not include mere words.

Access to LCTI’s CIS systems through school resources is a privilege, not a right. These, as well as the User accounts and information, are the property of LCTI, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. LCTI will cooperate to the extent legally required with other educational entities, social media sites, ISPs, local, state and federal officials in any investigation concerning or related to the misuse of the CIS systems, or other legal requests, whether criminal or civil actions.
It is often necessary to access User accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception, and to access the stored communication of User accounts for any reason in order to uphold this Policy, administrative regulations, the law and to maintain the system. Users have no privacy expectations in the contents of their personal files or any of their use of the LCTI’s CIS systems. **USERS HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE LCTI’S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE LCTI’S CIS SYSTEMS.** LCTI reserves the right to record, check, receive, monitor, track, log, access and otherwise inspect any or all CIS systems use and to monitor and allocate fileserver space. Users of the LCTI’s CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communication recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by LCTI and to the monitoring and allocating fileserver space. Passwords and message delete functions do not restrict the LCTI’s ability or right to access such communications or information.

**20 U.S.C. § 6777(c); 24 P.S. § 4610**

LCTI reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, LCTI operates and enforces Technology Protection Measure(s) that block or filter online activities of Minors on its Computers used and accessible to adults and students so as to filter or block Inappropriate Matter on the Internet. Inappropriate matter on the Internet as defined in this Policy. Measures designed to restrict adults’ and Minors’ access to material Harmful to Minors may be disabled to enable an adult or student (who has provided written consent from a parent or guardian) to access *bona fide* research, not within the prohibitions of this Policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law.

**20 U.S.C. § 6777(c); 24 P.S. § 4610**

Expedited review and resolution of a claim that the Policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of a written consent from a parent/guardian for a student, and upon the written request from an adult presented to the Supervisor of Technology and/or designee.

**20 U.S.C. § 6777(c); 24 P.S. § 4601**

The LCTI has the right, but not the duty, to inspect, review, or retain Electronic Communication created, sent, displayed, received or stored on and over the LCTI’s CIS systems and to monitor, record, check, track, log, access or otherwise inspect its CIS systems.
In addition, *in accordance with the law*, LCTI has the right, but not the duty, to inspect, review, or retain Electronic Communications created sent, displayed, received, or stored *on User’s* personal Computers, electronic devices, networks, Internet, Electronic Communications Systems, and in databases, files, software and media that contain LCTI programs, information and/or data.

Also, *in accordance with the law*, the LCTI has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored *on another entity’s* Computer or electronic device when Users bring and use another entity’s computer or electronic device to a LCTI location, event, or connect it to the LCTI network and/or systems, and/or that contains LCTI programs or LCTI data or information.

The above applies no matter where the use occurs whether brought onto LCTI property, to LCTI events, or connected to the LCTI network, or when using mobile computing equipment and telecommunications facilities in protected or unprotected areas or environments, directly from home, or indirectly through another social media or ISPs, as well as by other means. All actions must be conducted *in accordance with the law*, assist in the protection of the LCTI’s resources, insure compliance with this Policy, or other LCTI policies, regulations, rules, and procedures, social media and internet service providers terms, or local, state and federal laws.

LCTI reserves the right to restrict or limit usage of lower priority CIS systems and Computer uses when network and computing requirements exceed available capacity according to the following priorities:

1. **Highest** – uses that directly support the education of the students.
2. **Medium** – uses that indirectly benefit the education of the students.
3. **Lowest** – uses that include reasonable and limited educationally-related interpersonal communications and Incidental Personnel Use.
4. **Forbidden** – all activities in violation of this Policy, other LCTI policies, regulations, rules, procedures, ISP terms, and local, state and federal law.

LCTI additionally reserves the right to:

1. Determine which CIS systems’ services will be provided through LCTI resources.
2. Determine the types of files that may be stored on LCTI file servers and computers.

3. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, including e-mail, text message and other electronic communications.

4. Remove excess e-mail and other electronic communications, or files taking up an inordinate amount of file server disk space after a reasonable time.

5. Revoke User privileges, remove User accounts, or refer to legal authorities when violation of this and/or any other applicable LCTI policies, regulations, rules, and/or procedures occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, social media, vendor access, data breach, electronic communication devices and destruction of LCTI resources and equipment.

Due to the nature of the Internet as a global network connecting thousands of computers around the world, Inappropriate Matter as defined in this Policy, can be accessed through the network and Electronic Communications Systems. Because of the nature of the technology that allows the Internet to operate, LCTI cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of LCTI resources and will result in actions explained further in Consequences for Inappropriate, Unauthorized and Illegal Use section, found in the last section of this Policy and as provided in relevant LCTI policies, regulations, rules and procedures.

LCTI must publish a current version of this Policy so that all Users are informed of their responsibilities. A copy of this Policy, and the CIS Acknowledgement and Consent Form(s) must be provided to all Users, who must sign the LCTI’s Acknowledgement Form, either by electronic or written means.

Employees must be capable and able to use LCTI’s CIS systems and software relevant to the employee’s responsibilities.

4. Delegation of Responsibility

The Supervisor of Technology, and/or designee, will serve as the coordinator to oversee LCTI’s CIS systems and will work with other regional or state organizations as necessary to educate Users, approve activities, provide leadership for proper training for all Users in the use of the CIS systems and the requirements of this Policy, establish a system to ensure adequate supervision of the CIS systems, maintain executed User Acknowledgement and Consent Forms, and interpret and enforce this Policy.
Pol. 800

The Supervisor of Technology, and/or designee, will establish a process for setting-up individual and class accounts, set quotas for disk usage on the system, establish Records Retention and Records Destruction Policy (see Policy #800) and a Records Retention Schedule to include electronically stored information, and establish LCTI’s virus protection process.

Unless otherwise denied for cause, student access to the CIS systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within LCTI and LCTI CIS systems, and to abide by the rules established by LCTI, its ISP and local, state and federal laws.

47 U.S.C. § 254 (5)(B)(iii); 24 P.S. § 1303.1-A

Pol. 249

4. Guidelines

Access To The CIS Systems

1. The CIS systems’ accounts of Users must be used only by authorized owners of the accounts for authorized purposes.

2. An account will be made available according to a procedure developed by appropriate LCTI authorities.

3. CIS System - LCTI’s Acceptable Use of the Communications and Information Systems Policy, as well as other relevant LCTI policies, regulations, rules, and procedures, will govern use of LCTI’s CIS systems for Users.

4. Types of services include, but are not limited to:

   a. Internet - LCTI employees, students and Guests will have access to the Internet through LCTI’s CIS systems as needed.

   b. E-Mail and Text Messaging - LCTI employees may be assigned individual e-mail and text messaging accounts for work-related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Supervisor of Technology, and/or designee, and at the recommendation of the teacher who will supervise the students’ use of the e-mail service. Students and Guests may not be assigned text message accounts.
c. **Guest Accounts** - Guests may receive an individual Internet account with the approval of the Supervisor of Technology, and/or designee, if there is a specific LCTI-related purpose requiring such access. Use of the CIS systems by a Guest must be specifically limited to LCTI-related purpose and comply with this Policy, all other LCTI policies (including Vendor Access Policy), regulations, rules, and procedures, as well as ISP terms, and local, state and federal laws and may not damage LCTI’s CIS systems. A LCTI CIS Acknowledgement and Consent Form must be signed, and if the Guest is a Minor, a parent’s written signature also is required.

d. **Blogs** - Employees may be permitted to have LCTI-sponsored blogs after they receive training and the approval of the Supervisor of Technology and/or designee. All bloggers must follow the rules provided in this Policy, and all other applicable policies, rules and procedures of the LCTI, as well as ISP terms, and local, state, and federal laws.

e. **Web 2.0 Second Generation and Web 3.0 Third Generation Web-based Services** - Certain LCTI authorized Second Generation and Third Generation Web-based services, such as blogging, authorized social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies, and collaboration tools that emphasize online participatory learning (where Users share ideas, comment on one another’s project, plan, design, or implement, advance or discuss practices, goals, and ideas together, co-create, collaborate and share) among Users may be permitted by LCTI, however, such use must be approved by the Supervisor of Technology, and/or designee, followed by training authorized by LCTI. Users must comply with this Policy, as well as any other relevant policies, regulations, rules and procedures including the copyright, ISP terms, and local, state and federal laws during such use.

**Parental Notification And Responsibility**

LCTI will notify the parents/guardians about the LCTI CIS systems and the policies, regulations, rules and procedures governing their use. This Policy contains restrictions on accessing inappropriate Material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for LCTI to monitor and enforce a wide range of social values in student use of the Internet. Further, LCTI recognizes that parents and guardians bear primary responsibility for transmitting their particular set of family values to their children. LCTI will encourage
parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the LCTI’s CIS system. Parents/Guardians are responsible for monitoring their children’s use of LCTI’s CIS systems when they are accessing the systems from home.

**LCTI Limitation Of Liability**

LCTI makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through LCTI’s CIS systems will be error-free or without defect. LCTI does not warrant the effectiveness of Internet filtering. The electronic information available to Users does not imply endorsement of the content by LCTI, nor is LCTI responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. LCTI shall not be responsible for any damage Users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the Computers, network and Electronic Communications Systems. LCTI shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. LCTI shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to LCTI’s CIS systems. In no event shall LCTI be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the CIS systems.

**Prohibitions**

The use of LCTI’s CIS systems for illegal, inappropriate, unacceptable or unethical purposes by Users is prohibited. Such activities engaged in by Users are strictly prohibited and illustrated below. LCTI reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the CIS systems.

These prohibitions are in effect any time LCTI resources are accessed whether on LCTI property, at LCTI events, while connected to LCTI’s network, when using mobile commuting equipment, telecommunication facilities in protected and unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment.
Students are prohibited from visually possessing and using their personal computers and personal electronic communication devices, as defined in this Policy, on LCTI premises and property (including but not limited to, buses and other vehicles), at LCTI events or through connection to LCTI CIS systems, unless expressed permission has been granted by a teacher or administrator, who will then assume the responsibility to supervise the student in its use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its use. Students who are performing volunteer fire company, ambulance or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of their family, with notice and the approval of the school administrator, may qualify for an exemption of this prohibition. See LCTI Policy 237.

**General Prohibitions**

Users are prohibited from using LCTI CIS systems to:

1. Communicate about nonwork or non-school related matters, unless the employee’s use comports with the definition of Incidental Personal Use in this Policy.

2. Send, receive, view, download, store, access, print, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, sexually explicit or sexually suggestive. This includes but is not limited to, Visual Depictions. Examples include, taking, disseminating, transferring, or sharing Obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as, sexting, e-mailing, texting, among others). Nor may Users advocate the destruction of property.

3. Send, receive, view, download, store, access, print, distribute, or transmit Inappropriate Matter as defined in this Policy, and material likely to be offensive or objectionable to recipients.

4. Cyberbullying another individual or entity. See LCTI’s Bullying/Cyberbullying Policy # 249.

5. Access or transmit gambling information, or promote or participate in pools for money, including but not limited to, basketball and football or any other betting or games of chance.

6. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of Inappropriate matter in this Policy.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td>Send terroristic threats, hateful mail, harassing communications, discriminatory remarks and offensive or inflammatory communications.</td>
</tr>
<tr>
<td>8.</td>
<td>Participate in <em>unauthorized</em> Internet Relay Chats, instant messaging communications and Internet voice communications (online; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties. Students may not use IRCs unless approval has been granted by Supervisor of Technology and/or designee.</td>
</tr>
<tr>
<td>9.</td>
<td>Use in an illegal manner or to facilitate any illegal activity.</td>
</tr>
<tr>
<td>10.</td>
<td>Communicate through e-mail or text messages for non-educational purposes or activities, unless it is for Incidental Personal Use as defined in this Policy. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the “everyone” distribution list, building level distribution lists, all staff lists, or other e-mail distribution lists to offer personal items for sale is prohibited).</td>
</tr>
<tr>
<td>11.</td>
<td>Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable LCTI policies); conduct unauthorized fundraising or advertising on behalf of LCTI and non-LCTI organizations; engage in the resale of LCTI computer resources to individuals or organizations; or use LCTI’s name in any unauthorized manner that would reflect negatively on LCTI, its employees or students. <strong>Commercial purposes</strong> are defined as offering or providing goods or services or purchasing goods or services for personal use. LCTI acquisition policies will be followed for LCTI purchase of goods or supplies through the LCTI system.</td>
</tr>
<tr>
<td>12.</td>
<td>Engage in political lobbying.</td>
</tr>
<tr>
<td>13.</td>
<td>Install, distribute, reproduce or use copyrighted software on LCTI computers, or copy LCTI software to unauthorized Computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See Copyright Infringement in this Policy and LCTI’s Copyright Policy # 814 for additional information.</td>
</tr>
<tr>
<td>14.</td>
<td>Install Computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on LCTI computers is restricted to the Supervisor of Technology and/or designee.</td>
</tr>
</tbody>
</table>

Pol. 814
15. Encrypt messages using encryption software that is not authorized by LCTI from any access point on LCTI equipment or LCTI property. Users must use LCTI approved encryption to protect the confidentiality of sensitive or critical information in LCTI’s approved manner.

16. Access, interfere, possess, or distribute confidential or private information without permission of the LCTI’s administration. An example includes accessing other students’ accounts to obtain their grades, or accessing other employee’ accounts to obtain their personal information.

17. Violate the privacy or security of electronic information.

18. Send any LCTI information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of LCTI’s business, or educational interest.

19. Send unsolicited commercial electronic mail messages, also known as spam.

20. Post personal or professional web pages on the LCTI’s web site without administrative approval.

21. Posting anonymous messages.

22. Use the name of “Lehigh Career & Technical Institute” in any form in blogs, on LCTI Internet pages or web sites not owned or related to LCTI, or in forums/discussion boards, and social media sites, to express or imply the position of Lehigh Career & Technical Institute without the expressed, written permission of the Supervisor of Technology. When such permission is granted, the posting must state that the statement does not represent the position of LCTI.

23. Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/proxies or any web sites that mask the content the User is accessing or attempting to access.

24. Advocate illegal drug use, whether expressed or through a latent pro-drug message. This does not include a restriction of political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use.

25. Attempt to or obtain personal information under false pretenses with the intent to defraud another person.
26. Use location devices to invade a person’s privacy or to harm or put another person in jeopardy.

27. Plagiarize works that are found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as they were yours.

28. Post false statements or steal the identity of another person.

Access And Security Prohibitions

Users must immediately notify the Supervisor of Technology, and/or designee, if they have identified a possible security problem. Users must read, understand, provide a signed CIS Acknowledgement and Consent Form(s), and comply with this Policy that includes network, Internet usage, electronic communications, telecommunications, non-disclosure and physical and information security requirements. The following activities related to access to LCTI’s CIS systems, and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication.

2. Acquiring or attempting to acquire User IDs and passwords of another. Users are required to use unique strong passwords that comply with LCTI’s password, authentication and syntax requirements. Users will be held responsible for any misuse of Users’ names or passwords while the Users’ systems access were left unattended and accessible to others, whether intentional or through negligence.

3. Using or attempting to use Computer accounts of others. These actions are illegal, even with consent or if only for the purpose of “browsing”.

4. Altering a communication originally received from another person or Computer with the intent to deceive.

5. Using LCTI resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons. Such acts would include, but are not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity or being involved in a terroristic threat against any person or property.

6. Disabling or circumventing any LCTI security, program or device, for example, but not limited to, anti-spyware, anti-spam software and virus protection software or procedures.
7. Transmitting electronic communications anonymously or under an alias unless authorized by LCTI.

8. Accessing any web site that the LCTI has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social media, music and video download and gaming sites.

9. Installing or attaching keylogging devices, keylogging mechanisms or keylogging software of any kind.

Pol. 830

Users must protect and secure all electronic resources and information, data and records of the LCTI from theft and inadvertent disclosure to unauthorized individuals or entities at all times. If any User becomes aware of the release of LCTI information, data or records, the release must be reported to the Executive Director and/or designee immediately. See LCTI’s Data Breach Notification Policy # 830 for further information.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interference with, infiltration into, or disruption of the CIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of Computer “worms” and “viruses”, Trojan Horse trapdoor, robot, spider, crawler, program code, the sending of electronic chain mail, and the inappropriate sending of distasteful jokes or “broadcast” messages to large numbers of individuals or hosts. Users may not hack or crack the network or others’ Computers, whether by malware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the CIS systems, or the systems of others, or any component of the network, or strip or harvest information, or completely take over a person’s Computer or to “look around”. (See Policy # 830).

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the CIS systems for security vulnerabilities.

4. Attempting to alter any LCTI computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one’s level of authorization.
5. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any Computer, Electronic Communications Systems, or network services, whether wired, wireless, cable, virtual, cloud, cellular or by other means.

6. Connecting unauthorized hardware and devices to the CIS systems.

7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading unauthorized music and video files.

8. Intentionally damaging or destroying the integrity of LCTI’s electronic information.

9. Intentionally destroying the LCTI’s Computer hardware or software.

10. Intentionally disrupting the use of the CIS systems.

11. Damaging LCTI’s Computers, CIS systems, or networking equipment through the Users’ negligence or deliberate act, including but not limited to vandalism.

12. Failing to comply with requests from appropriate teachers or LCTI administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

Content Guidelines

Information electronically published on LCTI’s CIS systems shall be subject to the following guidelines:

1. Published documents including but not limited to audio and video clips or conferences, may not include a student’s date of birth, Social Security number, driver’s license number, financial information, credit card number, health information, phone number(s), street address, or box number, name (other than first name) or the names of other family members without parental consent.

2. Documents, web pages, electronic communications or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

3. Documents, web pages, electronic communications or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.
4. Documents, web pages and electronic communications, must conform to all LCTI policies, regulations, rules, and procedures.

5. Documents to be published on the Internet must be edited and approved according to LCTI policies, regulations, rules and procedures before publication.

**Due Process**

1. LCTI will cooperate with sending school districts’, the LCTI’s ISP rules, and local, state and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through LCTI’s CIS system.

2. If students or employees possess due process rights for discipline resulting from the violation of this Policy, they will be provided such rights.

3. LCTI may terminate the account privileges by providing notice to the User.

**Search And Seizure**

1. Users’ violations of this Policy, and any other LCTI policies, regulations, rules, or procedures, ISP terms, or the law may be discovered by routine maintenance and monitoring of the LCTI system, or any method stated in this Policy or pursuant to any legal means.

2. LCTI reserves the right, but not the duty, to inspect, review, or retain electronic communications created, sent, displayed, received, or stored on or over its CIS systems; to monitor, track, log and access or otherwise inspect; and/or report all aspects of its CIS systems. This includes items related to any personal Computers, network, Internet, Electronic Communications Systems, databases, files, software, and media that individuals may bring onto LCTI’s property, or to LCTI events, that were connected to the LCTI’s network, and/or that containing LCTI programs, or LCTI or Users’ data and information, in accordance with the law, in order to insure compliance with this Policy, other LCTI policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws to protect LCTI’s resources and to comply with the law.
USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER LCTI’S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF LCTI’S CIS SYSTEMS. LCTI reserves the right to record, check, receive, monitor, track, log access and otherwise inspect any or all CIS systems’ use and to monitor and allocate fileserver space.

3. Everything that Users place in their personal files should be entered with the knowledge and understanding that it is subject to review by a third party.

Copyright Infringement

1. Federal laws, cases, policies, regulations and guidelines pertaining to copyright will govern the use of material accessed through LCTI resources. Users must make a standard practice of requesting permission from the holder of the work, or complying with the Fair Use Doctrine, and/or complying with license agreements. Employees must instruct Users to respect copyrights, request permission when appropriate, and to comply with the Fair Use Doctrine and/or license agreements. Employees will respect and comply as well.

2. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. LCTI does not permit illegal acts pertaining to the copyright law. Therefore, any User violating the copyright law does so at their own risk and assumes all liability.

3. Violations of copyright law include, but are not limited to, making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over Computer networks, remixing or preparing mash-ups that violate the law, and deep-linking and framing into the content of others’ web sites. Further, the illegal installation of copyrighted software or files for use on LCTI’s Computers is expressly prohibited. This includes all forms of unlicensed software – shrink-wrap, clickwrap, broweswrap and electronic software downloaded from the Internet.

4. No one may circumvent a Technology Protection Measure that controls access to a protected work unless they are permitted to do so by law. No one may manufacture, import, offer to the public, or otherwise traffic in any technology, product, service, device, component or part that is produced or marketed to circumvent a technology protection measure to control access to a copyright protected work.
5. LCTI guidance on plagiarism will govern use of material accessed through LCTI’s CIS systems. Users must not plagiarize works that they find. Teachers must instruct students in appropriate research and citation practices. Users understand that use of the LCTI’s CIS systems may involve the LCTI’s use of plagiarism analysis software being applied to their works.

### Selection Of Material

1. LCTI policies, regulations, rules and procedures on the selection of materials will govern use of LCTI’s CIS systems.

2. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers must preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

### LCTI Web Site

LCTI has established and maintains a web site and will develop and modify its web pages that will present information about LCTI under the direction of the Supervisor of Technology and/or designee. Publishers must comply with this Policy, other LCTI’s policies, regulations, rules, procedures, ISP terms, and local, state and federal laws.

LCTI may limit its liability by complying with the Digital Millennium Copyright Act’s safe harbor notice and takedown provisions.

### Blogging

1. LCTI does not permit its employees, students or Guests to develop, implement, maintain and support a blog on behalf of the LCTI or for themselves using LCTI time, equipment and materials.
2. If an employee, student or Guest creates a blog with their own resources and on their own time, the employee, student or Guest may not violate the privacy rights of employees and students, may not use LCTI personal and private information/data, images, equipment, resources, and copyrighted material in their blog and may not disrupt the LCTI. See also LCTI’s Social Media Policy, and Social Media Administrative Regulations.

3. Contrary conduct may result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section of this Policy, and provided in relevant LCTI policies, regulations, rules and procedures.

4. No technical, graphic or editorial support will be provided to the employees by LCTI.

Safety And Privacy

1. To the extent legally required, Users of LCTI’s CIS systems will be protected from harassment or commercially unsolicited electronic communication. Any User who receives threatening or unwelcome communications must immediately send or otherwise provide them to the Supervisor of Technology and/or designee.

47 U.S.C. § 254

2. Users must not post personal contact information about themselves or other people on the CIS systems. Users may not steal another’s identity in any way, may not use spyware, malware, cookies, or other program code, keyloggers, and may not use LCTI or personal technology or resources in any way to invade another’s privacy. Additionally, User may not disclose, use, or disseminate confidential and personal information about students or employees, unless legitimately authorized to do so. Examples include, but are not limited to, revealing biometric data, student grades, Social Security numbers, dates of birth, home addresses, telephone numbers, school/work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports and resumes or other information relevant to seeking employment at LCTI.

3. If LCTI requires that data and information be encrypted, Users must use LCTI authorized encryption to protect their privacy and security.

4. Student Users by their use of the LCTI’s CIS systems, agree not to meet with someone they have met online unless they have parent(s)/guardian(s) consent.
5. Users must keep all LCTI, employee, and student information on/in LCTI’s and its contracted party’s systems/storage, unless permission is granted by the Supervisor of Technology for a student, an employee, or a Guest to place LCTI information in/on an alternate approved system/storage and LCTI has their information available to it. This means that employees, students, and Guests must not place LCTI information in system/storage beyond the control, access, protection, and safety of LCTI unless specific permission is granted in writing by the Supervisor of Technology and the student, employee and Guest agree to the LCTI’s terms and conditions.

Consequences For Inappropriate, Unauthorized And Illegal Use

General rules for behavior, ethics, and communications apply when using the CIS systems and information, in addition to the stipulations of this Policy, regulations, rules, procedures, ISP terms, and local, state and federal laws. Users must be aware that violations of this Policy or other LCTI policies, regulations, rules, procedures, or for unlawful use of the CIS systems, may result in the loss of CIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissal, expulsions, breach of contract and/or legal proceedings. This will be handled on a case-by-case basis. This Policy incorporates all other relevant LCTI policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, copyright, data breach, property, curriculum, terroristic threat, vendor access, student electronic device and harassment policies.

The User is responsible for damages to Computers, the network, equipment, Electronic Communications systems, and software resulting from accidental, negligent, deliberate and willful acts. Users will also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy, other LCTI related policies, regulations, rules, and procedures, ISP terms, and local, state and federal laws. For example, Users will be responsible for payments related to lost or stolen Computers and/or LCTI equipment and recovery and/or breach of the information and/or data contained on them.

Any and all costs incurred by the LCTI for repairs and/or replacement of software, hardware and data files and for technological consultant services due to any violation of this Policy, other LCTI policies, regulations, rules, and procedures, or ISP terms, or federal, state, or local law, shall be paid by the User who caused the loss.
Violations as described in this Policy, regulations, rules and procedures may be reported to LCTI, appropriate legal authorities, whether the ISP, local, state or federal law enforcement. Actions that constitute a crime under state and/or federal law could result in arrest, criminal prosecution and/or lifetime inclusion on a sexual offender’s registry. LCTI will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to LCTI’s CIS systems and resources and the User is subject to discipline.

References:

PA Consolidated Statutes Annotated – 18 Pa. C.S.A. § 5903, 6312

PA Child Internet Protection Act – 24 P.S. § 4601 et seq.

PA Bullying Act – 24 P.S. § 13-1303.1-A

PA – 18 Pa. C.S.A. § 6312; 24 P.S. § 4603, 4604


Digital Millennium Copyright Act 17 U.S.C. § 512, 1202


School Code – 24 P.S. § 1317.1

Board Policies, Administrative Regulations, Rules, and Procedures