

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS

BOARD ADOPTED APRIL 16, 2018

820 ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS

A. PURPOSE

1. To establish an Internet Systems Safety Policy (IST) and to provide permissible uses of the Carbon Lehigh Intermediate Unit's work place technology resources provided by Carbon Lehigh Intermediate Unit ("CLIU").

B. AUTHORITY

1. The Board directs the Management Information Systems ("MIS") department to provide electronic communication/information collection systems and voicemail systems that facilitate inter/intraoffice communication and/or information collection for conducting Carbon Lehigh Intermediate Unit business.

C. DEFINITIONS

1. **Users** Carbon Lehigh Intermediate Unit Staff Members, students enrolled at Carbon Lehigh Intermediate Unit site locations and any other individual given permission by the Carbon Lehigh Intermediate Unit Executive Director or his/her designee to access the work place CLIU technology resources.
2. **Technology Resources** means all Electronic Equipment and Computer Hardware, Computer Software, and Authorized Software owned, operated, and/or licensed by the CLIU.
3. **Electronic Equipment and Computer Hardware** includes but is not limited to servers, personal computers, printers, scanners, routers, hubs, storage media tape drives, flash drives, floppy diskettes, diskettes, hard drives, modems, network cards, laptops, cell phones, tablets, and all hardware accessories.
4. **Computer Software** includes but is not limited to all software applications, user accounts, operating systems, network operating systems, and all backup utility software, e-mail, web-sites, firewall, mobile applications and all software applications purchased and/or authorized for use on CLIU hardware and/or network. Network includes but is not limited to CLIU Network, Protocol, IP, IPX, SPX, TCP/IP, NT, UNIX, firewall network licenses, Internet, private public domain, e-mail, web-site, and all network browsers.
5. **Authorized Software** is a software application that has been submitted to and reviewed by the MIS department and deemed to be compatible with current systems and authorized by MIS to be installed, copied, downloaded, loaded, or ran on CLIU electronic equipment, computer hardware, and/or network.
6. **Electronic Mail** is the simultaneous electronic transfer of text messages, images, files, information or data to one or more parties via the intranet or Internet systems.

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS

BOARD ADOPTED APRIL 16, 2018

- 37 7. **Voice Mail** is the electronic transfer of voice messages via the telephone system.
- 38 8. **Internet Systems Access** is the ability to connect to the Internet systems and access, utilize and
39 manipulate data, images, material, files and information.
- 40 9. **Child Pornography** Any visual depiction, including any photograph, film, video, picture, or
41 computer-generate image or picture, whether made or produced by electronic, mechanical, or
42 other means, of sexually explicit conduct, where:
- 43 a. The production of such visual depiction involves the use of a minor engaging in sexually
44 explicit conduct;
- 45 b. Such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
- 46 c. Such visual depiction has been created, adapted, or modified to appear that an identifiable
47 minor is engaging in sexually explicit conduct; or
- 48 d. Such visual depiction is advertised, promoted, presented, described, or distributed in such a
49 manner that conveys the impression that the material is or contains a visual depiction of a
50 minor engaging in sexually explicit conduct.
- 51 10. **Harmful To Minors** Any picture, image, graphic image file or other visual depictions
- 52 a. taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or
53 excretion;
- 54 b. depicts, describes, or represents in a patently offensive way with respect to what is suitable
55 for minors, an actual or simulated sexual content, actual or simulated normal or perverted
56 sexual acts, or lewd exhibition of the genitals; and
- 57 c. taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

58
59 **D. ACCESS TO SYSTEM(S)**

- 60 1. Access to and use of the CLIU technology resources is a privilege granted solely to employees
61 who are provided an authorized user account or other individuals specifically granted permission
62 by the Carbon Lehigh Intermediate Unit Executive Director or his/her designee.
- 63 2. The Carbon Lehigh Intermediate Unit Executive Director or his/her designee shall be responsible
64 for implementing technology and procedures to determine whether the organization's work place
65 technology are being used for the purposes prohibited by law or for accessing sexually explicit
66 materials. The procedure shall include but not limited to:
- 67 a. Utilizing a technology protection measure that blocks or filters Internet systems access for
68 minors and adults to certain visual depictions that are obscene, child pornography, harmful to
69 minors with respect to use by minors, or determined inappropriate for use by minors by the
70 Board.

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS

BOARD ADOPTED APRIL 16, 2018

- 71 b. Maintaining and securing a usage log.
72 c. Monitoring online activities of minors.
- 73 3. The CLIU establishes that access to and use of the CLIU technology resources is a privilege and
74 not a right.
- 75 4. The CLIU reserves the right to revoke, remove or disable user privileges and/or accounts
76 temporarily or permanently at its sole discretion.
- 77 5. In order to be issued access and user privileges, an employee must read this policy and sign a user
78 agreement.
- 79 6. Employees may only access and use CLIU technology resources through their authorized user
80 account unless otherwise directed by a CLIU administrator.
- 81 7. Nothing in this policy shall prevent a Parent or Guardian from assisting his or her child with the
82 use of the CLIU's technology resources, or from monitoring a student's use of the CLIU's
83 technology resources in the student's home.

84

E. PERMISSIBLE USE

- 86 1. An Employee who is provided an authorized account or other person given permission by a
87 Carbon Lehigh Intermediate Unit Administrator may access CLIU technology resources for
88 official Carbon Lehigh Intermediate Unit business, so long as such use is:
- 89 a. Is performed in a professional and ethical manner as deemed by the CLIU in its sole
90 discretion;
- 91 b. Does not violate state or federal law;
- 92 c. Does not violate board policy;
- 93 d. Does not result in an infringement or violation upon any patents or copyrights;
- 94 e. Does not result in personal use involving significant use of CLIU resources, direct costs, or
95 any interference with the performance of CLIU designated duties, work, responsibilities or
96 data communication networks as deemed by the CLIU in its absolute discretion;
- 97 f. Does not result in commercial gain, private profit or local market competition with the CLIU
98 (This includes but is not limited to chain letters, solicitation of business or services, sales of
99 personal property, etc.);
- 100 g. Does not result in offering or providing goods or services or purchasing goods or services for
101 personal use;
- 102 h. Does not result in political lobbying, as defined by the state statute covering political
103 lobbying (Intermediate Unit employees may use the system to communicate with their
104 elected representatives and to express their opinion on political issues during break periods.);

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS

BOARD ADOPTED APRIL 16, 2018

- 105 i. Does not result in the sharing of confidential information about students and/or Carbon
106 Lehigh Intermediate Unit staff;
- 107 j. Does not result in accessing, creating, displaying, uploading, downloading, copying, sending,
108 storing, transmitting or distributing pornographic, obscene, sexually explicit, abusive,
109 harassing, lewd, offensive, threatening or hate data, images, material or literature;
- 110 k. Does not result in the accessing, creating, displaying, uploading, downloading, copying,
111 storing, sending, distributing or transmitting obscene, pornographic, abusive, sexually
112 explicit, hate, harassing, lewd, offensive or threatening language or voice messages;
- 113 l. Does not result in annoying or harassing an individual;
- 114 m. Does not result in using another's individual's account or identity, e.g., forging electronic or
115 voice mail;
- 116 n. Does not result in activity that the CLIU in its absolute discretion determines to be
117 unacceptable or inappropriate;
- 118 o. Does not result in access to obscene or pornographic material or child pornography;
- 119 p. Does not result in access by students and minors to material that is harmful to minors or is
120 determined in appropriate for minors in accordance with Board policy;
- 121 q. Does not result in intentional obtaining or modifying of files, and/or passwords, and data
122 belonging to other users;
- 123 r. Does not result in disruption of the work of other users; and
- 124 s. Does not result in disruption, modification, abuse or unauthorized access to network
125 hardware, software, and files.

126
127 **F. STATUS OF COMMUNICATIONS AND/OR INFORMATION**

- 128 1. Communications, messages, data, images, material, literature and/or information accessed,
129 created, displayed, saved, sent, received, downloaded, uploaded, copied, stored, distributed and/or
130 transmitted using the electronic mail, Internet systems or voice mail are the property of the
131 Carbon Lehigh Intermediate Unit and are not to be considered private property.
- 132 2. The CLIU's Network records all electronic transfers of information, communications, data,
133 images, material and/or literature accessed, created, displayed, uploaded, downloaded, copied,
134 stored, sent, transmitted and/or distributed using the electronic mail and/or Internet systems.
- 135 3. All information transmitted and received via the internet as well as any files stored on CLIU
136 technology resources may be inspected at any time for any reason. The CLIU may decrypt and
137 inspect encrypted internet traffic and communications to ensure compliance with this policy.

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS
BOARD ADOPTED APRIL 16, 2018

- 138 4. The CLIU reserves the right to record, review, store and disclose all communications, messages,
139 data, images, material, literature and/or information to, inter alia, ascertain compliance with
140 acceptable use policies at any time the CLIU deems. The MIS Department may delete files
141 deemed to be beyond managerial storage levels.

142
143 **G. SECURITY**

- 144 1. System security is protected through the use of passwords. Failure to adequately protect or
145 update passwords could result in unauthorized access to personal or CLIU files. To protect the
146 integrity of the system, the following guidelines shall be followed:
- 147 a. Users shall not reveal their passwords to anyone other than a designated person(s) so
148 identified by the Carbon Lehigh Intermediate Unit Executive Director (Executive Director) or
149 the Executive Director's designee.
- 150 b. Users are not to use a computer that has been logged in under another student's or
151 employee's name.
- 152 c. Any user identified as a security risk or having a history of problems with other computer
153 systems may be denied access to the network.

154
155 **H. SAFETY**

- 156 1. The CLIU is committed to providing quality and filtered network access. A user who receives
157 threatening or unwelcome communications shall report such immediately to a supervisor,
158 director, or administrator. Users shall not reveal personal information to other users on the
159 network, including but not limited too, chat rooms, e-mail, Internet systems, etc.
- 160 2. Any computer/server utilized within the CLIU network by students or staff shall be provided with
161 Internet systems blocking/filtering protection measures.
- 162 3. Internet systems safety measures shall effectively address the following:
- 163 a. Control of access by minors to inappropriate matter on the Internet systems and World Wide
164 Web.
- 165 b. Safety and security of minors when using electronic mail, chat rooms, and other forms of
166 direct electronic communications.
- 167 c. Prevention of unauthorized online access by minors, including "hacking" and other unlawful
168 activities.
- 169 d. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- 170 e. Restriction of minor's access to materials harmful to them.

820

ACCEPTABLE USE OF ELECTRONIC SYSTEMS/COMMUNICATIONS
BOARD ADOPTED APRIL 16, 2018

- 171 f. The Carbon Lehigh Intermediate Unit Executive Director or his/her designee may disable the
172 technology protection measure concerned, during use by an adult, to enable access for bona
173 fide research or other lawful purposes.
- 174 4. Student Safety – When posting information to the web, it is important to consider that anyone can
175 view that information. Special care should be taken when posting student information to the web:
- 176 a. No web page content should allow people accessing the page to contact any student directly.
- 177 b. If a student’s picture or project is to be published on the Internet or transmitted outside of the
178 CLIU, a signed parent/guardian permission release form is required.
- 179 c. Public WebPages and other forms of electronic data transferred outside of the CLIU’s digital
180 network shall not contain any personal student information. Schools should proceed with
181 caution and sensitivity in this area.
- 182 d. Student photographs, drawings, and written work that are published on a class or school page
183 may NOT contain any personal information that can be linked to the student.
- 184 e. Employees may use first names and last initials or other codes, such as the teacher’s name
185 and a number for each student within the web page and with all file names.
- 186 5. The Carbon Lehigh Intermediate Unit recognizes the importance of teaching acceptable use and
187 online safety to students. The Carbon Lehigh Intermediate Unit’s Special Programs and Services
188 Department will provide instruction to students, enrolled at a CLIU site based program, about
189 appropriate online behavior, including interacting with other individuals on social networking
190 web sites and in chat rooms and cyber bullying awareness and response.

191
192 **I. SANCTIONS FOR VIOLATION OF POLICY**

- 193 1. Access to and use of CLIU technology resources for anything other than the permissible use
194 stated in this policy whether through ignorance, negligence, or deliberate disregard may result in
195 the revocation of privileges and/or user accounts and/or disciplinary action up to and including
196 termination. In addition, illegal use of CLIU technology resources will be reported to the
197 appropriate legal authorities.