EASTCONN TECHNOLOGY POLICY

Standards of Responsible Technology Use

All staff and students in EASTCONN schools must adhere to the following standards of responsible use:

- EASTCONN may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on EASTCONN servers (internal or cloud-based) will always be private.
- Students and Staff are responsible at all times for their use of EASTCONN's electronic communication system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.
- Students and Staff must log in and use the EASTCONN filtered wireless network during the school day on personal electronic devices.
- Students and Staff must not access, modify, download, or install computer programs, files, or information belonging to others.
- Students and Staff must not waste or abuse school resources through unauthorized system use (e.g. playing online games, downloading music, watching video broadcasts, participating in chat rooms, etc.)
- Students must not alter computers, networks, printers or other equipment except as directed by a staff member.
- Technology, including electronic communication, should be used for appropriate educational purposes only and should be consistent with the educational objectives of EASTCONN.
- Students and Staff must not release personal information on the Internet or electronic communications.
- If a student finds an inappropriate site or image, he or she must immediately minimize the program and contact the instructor.
- Students and Staff must not create/publish/submit or display any materials/media that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal and should report any instances encountered.

- Use of cameras (in-phone or otherwise), speaker-phone features, video calls, live video or audio transmission, or recordings of any sort are prohibited in restrooms, dressing rooms, locker rooms, or other areas where there is an expectation of privacy. Cameras may be used by Staff to document the condition of the room if the room is clear of all other individuals.
- Students and Staff shall adhere to all laws and statutes related to issues of copyright or plagiarism.
- Violation of any of these standards may result in suspension of computer use, Internet privileges and/or other disciplinary action.

Unacceptable technology use by EASTCONN students and staff includes but is not limited to:

- Personal gain, commercial solicitation and personal compensation of any kind;
- Liability or cost incurred by EASTCONN;
- Downloading, installation and use of unauthorized applications without permission or approval from programs leads; making available for student use any network service or software not compliant with CTGS statues pertaining to student data privacy;
- Removing inventory tags or obfuscating serial numbers;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
- Unauthorized access to other EASTCONN computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks; including after school hours and weekends. Schools officials may access emails of students for investigatory purposes.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;
- Attaching unauthorized equipment to the EASTCONN network;
- Using EASTCONN technology to support or oppose ballot measures, candidates, political or social policy or otherwise espouse or promulgate personal perspectives and viewpoints on these issues;

- Defacing any EASTCONN-owned device with stickers, stencils, markers, etching, or other marks, especially those supporting or opposing ballot measures, candidates, political or social policy or otherwise espousing or promulgating personal perspectives and viewpoints on these issues;
- Violation of any of these standards may result in suspension of computer use, Internet privileges and/or other disciplinary action.

Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or EASTCONN web site unless the appropriate permission has been verified according to EASTCONN policy.
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

Definitions

1. **Obscene** is to be determined by the following standards:

   - Whether the average person, applying contemporary community standards, would find the work, taken as a whole, appeals to the prurient interest;
   - Whether the work depicts sexual conduct in an offensive way; and
   - Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

2. Child Pornography, as defined in 18 U.S.C. 2256 means any visual depiction, including any photograph, film, video, picture, computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

- such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;

- such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or

- such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

3. Material **"Harmful to Minors"** is any picture, graphic image file or other visual depiction that:

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

- depicts, describes, or represents, in a patently offensive way with respect to what is suitable to minors, an actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

- taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

Filtering and Monitoring Responsibilities

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;

- Any attempts to defeat or bypass EASTCONN's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to EASTCON's browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;

- E-mail inconsistent with the educational and research mission of EASTCONN will be considered SPAM and blocked from entering EASTCONN e-mail boxes;
- EASTCONN will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to EASTCONN computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of EASTCONN; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

Filtered Topics and Content

EASTCONN access internet content through the Connecticut Education Network, and accepts its baseline recommendations for internet content filtering. Additional content may be filtered based on the following criteria:

Nudity/Pornography

- Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
- Provocative semi-nudity (e.g., lingerie models)
- Sites which contain pornography or links to pornographic sites
- Exceptions: Classical nudity (e.g., Michelangelo)

Sexuality

- Sites which contain material of a mature level (re: elementary/middle school levels)
- Images or descriptions of sexual aids
- Descriptions of sexual acts or techniques
- Sites which contain inappropriate personal ads
- Sites which solicit sexual contact

Violence

- Sites which promote violence
- Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
- Graphic autopsy or crime-scene images

Crime

- Information of performing criminal acts (e.g., drug or bomb making, computer "hacking")
- Illegal file archives (e.g., software piracy)

Drug Use

- Sites which promote the use of illegal drugs
- Material advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
- Materials which promote abuse of any drugs or alcohol
- Exceptions: Material with valid educational use (e.g., drug-use statistics)

Tastelessness

- Images or descriptions of excretory acts (e.g., vomiting, urinating)
- Graphic medical images outside of a medical context
- Exception: Graphic medical images within a medical context

Language/Profanity

- Passages/Words too coarse to be softened by the word filter
- Profanity within images/sounds/multimedia files
- Adult humor; (e.g., inappropriate for the age/grade level of the persons accessing the material)
- NOTE: The focus is on American English, but profanity in other languages or dialects is blocked if brought to our attention.

Discrimination/Intolerance

- Material advocating discrimination (e.g., forms of intolerance and/or bigotry such as racial, goods, sexual orientation, disability, national origin, color or religious discrimination)
- Sites which promote intolerance, hate, or discrimination

Interactive Mail/Chat

- Sites which contain or allow inappropriate e-mail correspondence
- Sites which contain or allow inappropriate chat areas

Inappropriate Banner Advertising

- Advertisements containing inappropriate images

Gambling

- Sites which allow or promote online gambling

Illegal Weapons

- Sites which promote illegal weapons

For Agencies participating in the federal E-Rate program:

The Agency recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

Information Security

The Board of Directors recognizes the need for procedures to minimize the EASTCONN's exposure to information security threats.

- Access to EASTCONN information services shall not extend beyond last day of employ for staff.
- Access to EASTCONN information services shall not extend beyond the last day of enrollment for students.
- Immediate supervisors will notify Technology Solutions a minimum of 3 days prior to the last day of employment of any departing staff member.
- The Executive Director or designee may mandate annual training on information security as a requirement for continued network and internet access.

The Board of Directors recognizes that although EASTCONN provides devices for student use in the school setting, students will necessarily bring their personal devices into school given the increasing dependence on devices for personal communication and organization. Given this, this section describes the expectations of student behavior in the use of these devices.

Definition of "Device"

A "device" as part of this protocol is a piece of privately owned and/or portable electronic handheld technology that includes emerging mobile communication systems and smart technologies, laptops and netbooks, and any technology that can be used for wireless internet access, word processing, image capture/recording, sound recording and information transmitting, receiving, and storing.

For purposes of BYOD/BYOT a "device" means a privately owned wireless and/or portable electronic hand held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, portable internet devices, Personal Digital Assistants (PDAs), hand held entertainment systems or portable information technology systems that can be used for word processing, wireless internet access, image capture/recording, sound recording and information transmitting/receiving/storing.

Internet

- The only internet gateway that may be accessed by K-12 students while in EASTCONN schools and programs is the one provided by EASTCONN. This includes access through EASTCONN wireless and wired services through CEN and EASTCONN provided wireless access points. Any device brought to EASTCONN will not be permitted to use outside internet sources.

- Personal devices with enabled non-EASTCONN provided internet access, such as but not limited to cell phones/cell network adapters, are not permitted to be used to access outside internet sources at any time.

Security and Damages

- Responsibility to keep the device secure rests with the individual owner. EASTCONN is not liable for any device stolen or damaged on campus. If a device is stolen or damaged, it will be handled through the administrative office as other personal items that are stolen or damaged. It is recommended that skins, decals, and other custom touches be used to identify physically a student's device from others. Additionally, protective cases for technology are encouraged.

Bring Your Own Device/Technology Student and Parent Agreement

- The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his/her electronic device while at school. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole.
- Students and parents/guardians bringing devices to school or other EASTCONN sponsored activity must adhere to the Student Code of Conduct, as well as all applicable Board policies, particularly the Computer Acceptable Use policy.
- The use of these devices, as with any personally owned device, is strictly up to the building or program administrator and teacher.

Teachers' Role in Supporting Students' Personal Devices

Teachers are facilitators of instruction in their classrooms. Therefore, they will not spend time on fixing technical difficulties with students' personal devices in the classrooms. They will educate and provide guidance on how to use a device and troubleshoot simple issues, but they will not provide technical support. This responsibility resides at home with parents/guardians.

- Teachers may communicate information regarding educational applications and suggest appropriate tools that can be downloaded to personal devices at home. Parents will need to assist their younger children with downloads if they wish to follow teachers' suggestions. No applications are to be downloaded at school.
- Teachers are to closely supervise students to ensure appropriate use of technology in the classrooms.
- It is understood that not every student has his/her own electronic device. To ensure equal accessibility to technology resources, teachers will provide students with technology available within the school.
- The use of these student personal devices, as with any personally owned device, is strictly up to the teacher.

Principals' or Program Leaders' Role

- Principals and Program Leads shall notify all students, parents, and staff of the components of this policy that pertain to students.
- Any specific school or program policies, rules, or guidelines will be consistent with this policy

Operating Principles for Use of Personal Devices on School Campus

- Devices cannot be used during assessments, unless otherwise directed by a teacher.
- Students must immediately comply with teachers' requests to shut down devices or close the screen. Devices must be in silent mode and put away when asked by teachers.
- Students are not permitted to transmit or post photographic images/videos of any person on campus on public and/or social networking sites.
- Personal devices must be charged prior to bringing them to school and run off their own batteries while at school.
- To ensure appropriate network filters, students will only use EASTCONN's wireless connection in school and will not attempt to bypass the network restrictions by using any external wireless network.
- Students must be instructed that bringing devices on campus or infecting the network with a virus, Trojan, or program designed to damage, alter, destroy, alter, or provide

access to unauthorized data or information is in violation of EASTCONN's Acceptable Use Policy and will result in disciplinary actions.

- EASTCONN has the right to collect and examine any device that is suspected of causing problems or is the source of an attack or virus infection.
- Students must be instructed that possessing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of the Acceptable Use Policy and will result in disciplinary actions.
- Students can only access files on the computer or Internet sites which are relevant to the classroom curriculum and suggested by a teacher.
- Printing from personal devices is not permitted at school.
- Students are not to physically share their personal devices with other students, unless approved in writing by their parent/guardian.
- Personal devices may not be used to cheat on assignments, tests or for non-instructional purposes, such as making personal phone call and text/instant messaging.
- Personal devices may not be used to send inappropriate e-messages during the school day.
- Personal devices may be confiscated by staff and held secure during the school day.

Limitation of Liability

- EASTCONN will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions.
- EASTCONN will not be responsible for unauthorized financial obligations resulting from the use of, or access to, EASTCONN's computer network or the Internet.
- EASTCONN will not be responsible for inadvertently exposing students or staff to inappropriate content due to failures of filtering services or other related failures.

Social Media Publishing

The Board of Directors allows EASTCONN and schools within EASTCONN to create and maintain Web sites or use Social Media outlets for educational purposes. Web site and Social Media are potential avenues for educating, providing information, communicating and expressing creativity. EASTCONN and individual school websites shall be used to share information about school curriculum and instruction, school-authorized activities, and other information relating to our schools and our mission. Websites shall also provide instructional resources for staff and students.

- The content of materials published on websites should be professional quality and consistent with the education mission of the school system. Websites shall follow standards for ethical behavior in regard to information and technology by showing respect for the principles of intellectual freedom, intellectual property rights and the responsible use of information and technology. Pages shall reflect an understanding that both internal and external audiences will be viewing the information.
- Any pages or links representing EASTCONN shall follow guidelines and responsibilities pertaining to content standards, student records, copyright, and technical standards which are contained in the administrative regulations which accompany this policy

Guidelines for Internet or Cloud-based Services

The Board of Directors recognize the benefits of using Internet or Cloud-based services in some circumstances.

Use of these services should adhere to the following guidelines:

- EASTCONN staff require written approval from the Executive Director or designee to use any non-EASTCONN provided internet-based service for the storage or any student-related information to assure compliance with CTGS Student Data Privacy requirements. This includes services used by staff that may purposefully or inadvertently store student information and services used directly by students and required for program participation.

- EASTCONN staff require written approval from the Executive Director or designee to use any non-EASTCONN provided internet-based service for file storage, file delivery or communications to assure compliance with EASTCONN data-retention requirements and data back-up procedures.

LEGAL REFERENCES

Connecticut General Statues

1-19(b)(11) Access to public records. Exempt records.

1-213 Access to public records. Exempt records.

10-15b Access of parent or guardians to student's records.

10-234aa through 10-234dd colloq. “Student Data Privacy”.

10-209 Records not to be public.

10-233j Student possession and use of telecommunications devices.

11-8a Retention, destruction and transfer of documents.

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

31-48d Employees engaged in electronic monitoring required to give prior notice to employees.

46b-56 (e) Access to Records of Minors.

53a-182 Obstructing free passage: Class C misdemeanor.

53a-182b Harassment in the first degree: Class D felony. (as amended by PA 95-143)

53a-183 Harassment in the second degree: Class C misdemeanor.

53a-250 Definitions.

Connecticut Regulations

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)- parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

Federal Law and Regulations

Electronic Communications Privacy Act, 18 U.S.C. 2510-2522

20 U.S.C. 254 Children’s Internet Protection Act of 2000.

20 U.S.C. Section 6777, No Child Left Behind Act.

20 U.S.C. Education Provisions Act, as amended, added by section 513 of P.L. 93-568, codified

47 U.S.C. Children's Online Protection Act of 1998.

at 20 U.S.C.1232g.).

HR 4577, Fiscal 2001 Appropriations Law (contains Children's Internet Protection Act).

Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21st Century Act.

Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.

U.S. Const. Amend. I.

Case Law

Bethel School Agency v. Fraser, 478 US 675 (1986).

Board of Directors v. Pico, 457 U.S. 868 (1988).

Eisner v. Stamford Board of Directors, 440 F. 2d 803 (2nd Cir 1971).

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General

Ginsberg v. New York, 390 U.S. 629, at 642, n.10 (1968).

Hazelwood School Agency v. Kuhlmeier, 484 U.S. 620, 267 (198841.323.

Hazelwood School Agency v. Kuhlmeier, 484 U.S. 260, 108 S Ct 562 (1988).

Reno v. ACLU, 521 U.S. 844 (1997).

Tinker v. Des Moines Independent Community Dist., 393 US 503, (1969).

Trachtman v. Anker, 563 F. 2d 512 (2nd Cir. 1977) cert. denied, 435 U.S. 925 (1978)

Policy Adopted: August 23, 2022