EAST STROUDSBURG AREA SCHOOL DISTRICT
ACCEPTABLE USE OF COMMUNICATIONS AND INFORMATION (CIS) SYSTEMS
ADMINISTRATIVE REGULATION #815

This Administrative Regulation #815 is intended to accompany the East Stroudsburg Area School District Acceptable Use of Communications and Information (CIS) Systems Policy #815. Policy # 815 is incorporated into and must be read with this Administrative Regulation. Terms used in this Administrative Regulation are defined in Policy #815.

Table of Contents

Introduction

Users must practice proper etiquette, School District ethics, and agree to the requirements of the Acceptable Use of Communications and Information (CIS) Systems Policy #815, this Administrative Regulation, and other School District relevant policies, regulations, rules, and procedures.

Prohibitions

The use of the East Stroudsburg Area School District'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 in Policy #815 and below. The School District reserves the right to determine if any activity not appearing in the lists constitute an acceptable or unacceptable use of the CIS systems.

The prohibitions are in effect any time School District resources are accessed whether on School District property, through the East Stroudsburg Area School District Virtual Academy, at School District events, while connected to the School District'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 a User uses their own equipment. Students must also comply with the School District's Electronic Devices Policy, # 237.

General Prohibitions

Users are prohibited from using School District CIS systems to:

1. Communicate about non-work or non-school related matters unless the employees' use comports with the definition of Incidental Personal Use in Policy #815.

2. Send, receive, view, upload, download, store, access, print, distribute, or transmit material that is Harmful to Minors, indecent, Obscene, pornographic, Child Pornographic, terroristic, sexually explicit, 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, upload, download, store, access, print, distribute, or transmit Inappropriate Matter as defined in Policy #815, and material likely to be offensive or objectionable to recipients.

4. Cyberbullying another individual or entity. See School District Bullying/Cyberbullying Policy 249. 24 P.S. § 13-1301.1-A.

5. Gang up on a victim or target him/her or make him/her the subject of ridicule or aggression.

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

7. 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 Policy # 815.

8. Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive, profane, or inflammatory communications.

9. Participate in unauthorized Internet Relay Chats, newsgroups, 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 must obtain consent from their teacher to use IRC's, however even with such consent they may not

use instant messaging or text messaging. Employees may only use instant messaging and text messaging if consent was obtained from the Director of Technology, and/or designee.

10. Use in an illegal manner or to facilitate any illegal activity.

11. Communicate through e-mail or text messages for non-educational purposes or activities, unless it is for Incidental Personal Use as defined in Policy #815. 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, or other e-mail distribution lists to offer personal items for sale is prohibited).

12. Engage in commercial, for-profit, or any business purposes, (except where such activities are otherwise permitted or authorized under applicable School District policies); conduct unauthorized fundraising or advertising on behalf of the School District and non-School District organizations; engage in the resale of School District Computer resources to individuals or organizations; or use the School District's name in any unauthorized manner that would reflect negatively on the School District, its employees, or students. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. School District acquisition policies must be followed for School District purchase of goods or supplies through the School District system.

13. Engage in political lobbying.

14. Install, distribute, reproduce or use unauthorized copyrighted software on School District Computers, or copy School District software to unauthorized Computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright. See the Copyright Infringement section in Policy #815, and the School District's Copyright Policy #814 for additional information.

15. Install Computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on School District Computers is restricted to the Director of Technology, and/or designee.

16. Encrypt messages using encryption software that is not authorized by the School District from any access point on School District equipment or School District property. Users must use School District approved encryption to protect the confidentiality of sensitive or critical information in the School District's approved manner.

17. Access, interfere, possess, or distribute confidential or private information without permission of the School District's administration. An example includes accessing other students' accounts to obtain their grades, or accessing other employees' accounts to obtain information.

18. Violate the privacy or security of electronic information.

19. Send any School District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the School District's business or educational interest.

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

21. Post personal or professional web pages on the School District's website without administrative approval.

22. Post anonymous messages.

23. Use the name of the "East Stroudsburg Area School District" in any form in blogs, on School District internet pages or websites, on websites not owned or related to the School District, or in forums/discussion boards, and social networking websites, to express or imply the position of the School District without the expressed, written permission of the Superintendent, and/or designee. When such permission is granted, the posting must state that the statement does not represent the position of the School District.

24. Bypass or attempt to bypass internet filtering software by any method including, but not limited to, the use of anonymizer/proxies or any websites that mask the content the User is accessing or attempting to access.

25. 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.

26. Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person.

27. Use location devices to invade a person's privacy or to harm or put another person in jeopardy.

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

29. Post false statements, or assume the identity of another person.

Access and Security Prohibitions

Users must immediately notify the Director of Technology, and/or designee, if they have identified a possible security problem. Users must read, understand, and submit a signed CIS Acknowledgement and Consent Form(s), and comply with the School District's Policy #815, and this administrative regulation, that include network, internet usage, Electronic Communications, telecommunications, non-disclosure, and physical and information security requirements. The

following activities related to access to the School District'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/or passwords of another. Users are required to use unique strong passwords that comply with the School District's password, authentication and syntax requirements. Users will be held responsible for the result of any misuse of Users' names or passwords while the Users' systems access were left unattended and accessible to others, whether intentional or, whether 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 School District 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 not be 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 School District 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 the School District.

8. Accessing any website that the School District has filtered or blocked as unauthorized. Examples include, but are not limited to, unauthorized social networking, music download, and gaming sites.

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

Users must protect and secure all electronic resources and information data and records of the School District from theft and inadvertent disclosure to unauthorized individuals or entities at all times. If any User becomes aware of the release of School District information, data or records, the release must be reported to the Superintendent, and/or designee, immediately. See the School District's Data Breach 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, and other program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts. Users may not hack or crack the network or others' Computers, whether by 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."

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 School District 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, 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 files.

8. Intentionally damaging or destroying the integrity of the School District's electronic information.

9. Intentionally destroying the School District's Computer hardware or software.

10. Intentionally disrupting the use of the CIS systems.

11. Damaging the School District's Computers, CIS systems, 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 School District administrators to discontinue activities that threaten the operation or integrity of the CIS systems.

Content Guidelines

Information electronically published on the School District'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 School District policies, regulations, rules, and procedures.

5. Documents to be published on the internet must be edited and approved according to School District policy #815.1 Website Development and procedures before publication.
Due Process

The School District will cooperate with the ISPs, and local, state, and federal officials in investigations concerning or relating to any illegal activities conducted through the School District's CIS systems.

If students or employees possess due process rights for discipline resulting from the violation of Policy # 815 and this Administrative Regulation, they will be provided such rights.
The School District may terminate account privileges by providing notice to the Users.

Search And Seizure

Users' violations of Policy #815, this Administrative Regulation, any other School District policies, regulations, rules, or procedures ISP terms, or the law may be discovered by routine maintenance and monitoring of the School District CIS system, or any method stated in Policy #815 and this Administrative Regulation, or pursuant to any legal means.

The School District reserves the right, but not the duty, to inspect, review, or retain Electronic Communications created, sent, displayed, received, or stored on and over its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or report all aspects of its CIS systems. This includes items related to any personal Computers, network, Internet, Electronic

Communication Systems, databases, files, software, and media that individuals may bring onto School District property, or School District events, that were connected to the School District's network, and/or that contain School District programs, or School District or Users' data and information, all pursuant to law, in order to insure compliance with Policy #815, this Administrative Regulation, and other School District policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws to protect the School District'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 THE SCHOOL DISTRICT'S CIS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE SCHOOL DISTRICT'S CIS SYSTEMS. The School District 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.

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

Selection of Material

School District policies on the selection of materials will govern use of the School District's CIS systems.

When using the internet for class activities, teachers must 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 websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers must provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers must 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.

Etiquette

Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:

1. Be polite. Do not become abrasive in messages to others. General School District rules and policies for behavior and communicating apply.

2. Use appropriate language. Do not swear or use vulgarities or other inappropriate language.

3. Do not reveal the personal addresses or telephone numbers of others.

4. Recognize that generally electronic communications are not private or confidential.

5. Do not use the internet or electronic communications in any way that would interfere with or disrupt their use by other Users.

6. Consider all communications and information accessible through the School District's ISP to be the property of the School District.

7. Do not order any materials or use credit cards while using the School District's computers.

8. Respect the rights of other Users to an open and hospitable technology environment, regardless of race, sexual orientation, color, religion, national origin, gender, creed, ethnicity, age, marital status, political beliefs, or disability status. Policy 218.

Wearable Technology

Wearable technology such as earbuds/earphones are prohibited at all times during the school day unless prior permission has been granted by the individual classroom teacher and/or building administration. For educational and safety reasons students cannot cover or plug earbuds/earphones into both ears during the school day to ensure that one can hear directives and/or announcements at all times.

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
U.S. Copyright Law – 17 U.S.C. § 101 et seq.
Digital Millennium Copyright Act 17 U.S.C. § 512, 1202
United States Code – 18 U.S.C. § 1460, 2246, 2252, 2256; 47 U.S.C. § 254
Enhancing Education Through Technology Act of 2001 – 20 U.S.C. § 6777
Federal Children's Internet Protection Act – 47 U.S.C. § 254
Board Policies, Administrative Regulations, Rules, and Procedures