Regulation #4150
Employee Use of District's Computer Systems

Introduction

Computers, computer networks, electronic devices, Internet access, and electronic messaging systems are effective and important technological resources. The Board of Education (the "Board") has installed computers and a computer network(s), including Internet access and electronic messaging systems, on Board premises and may provide electronic devices that can access the network(s) and/or have the ability to send and receive messages with an operating system or network communication framework. Devices include but are not limited to personal computing devices, cellular phones, copiers, Smartphones, work phones, network access devices, radios, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices. Electronic messaging systems include mobile, chat, and instant message; cloud collaboration platforms, including internal chat, peer-to-peer messaging systems, and draft email message transfer; and products that have the ability to create duration-based or subjective removal of content, such as Snapchat, and security focused platforms, such as Signal. The Board's computers, computer networks, electronic devices, Internet access, and electronic messaging systems are referred to collectively as "the computer systems" and are provided in order to enhance the educational and business operations of the district. In these regulations, the computers, computer network, electronic devices, Internet access and email system are referred to collectively as "the computer systems."

These computer systems are business and educational tools. As such, they are made available to employees of the district for district-related educational and business purposes. *All users of the computer systems must restrict themselves to appropriate district-related educational and business purposes*. Incidental personal use of the computer systems may be permitted solely for the purpose of email transmissions and similar communications, including access to the Internet on a limited, occasional basis. Such incidental personal use of the computer systems is subject to all rules, including monitoring of all such use, set out in these regulations. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

These computer systems are expensive to install, own and maintain. Unfortunately, these computer systems can be misused in a variety of ways, some of which are innocent and others deliberate. Therefore, in order to maximize the benefits of these technologies to the district, our employees and all our students, this regulation shall govern *all* use of these computer systems.

Monitoring

It is important for all users of these computer systems to understand that the Board, as the owner of the computer systems, reserves the right to monitor the use of the computer systems to ensure that they are being used in accordance with these regulations. The Board

intends to monitor in a limited fashion, but will do so as needed to ensure that the systems are being used appropriately for district-related educational and business purposes and to maximize utilization of the systems for such business and educational purposes. The Superintendent reserves the right to eliminate personal use of the district's computer systems by any or all employees at any time.

The system administrator and others managing the computer systems may access electronic messaging systems (including email) or monitor activity on the computer system or electronic devices accessing the computer systems at any time and for any reason or no reason. Typical examples include when there is reason to suspect inappropriate conduct or there is a problem with the computer systems needing correction. Further, the system administrator and others managing the computer systems can access or monitor activity on the systems despite the use of passwords by individual users, and can bypass such passwords. In addition, review of emails, messages or information stored on the computer systems, which can be forensically retrieved, includes those messages and/or electronic data sent, posted and/or retrieved using social networking sites, including, but not limited to, Twitter, Facebook, LinkedIn, Instagram and YouTube.

Notwithstanding the above and in accordance with state law, the Board may not: (1) request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing a personal online account; (2) request or require that an employee authenticate or access a personal online account in the presence of a Board representative; or (3) require that an employee invite a supervisor employed by the Board or accept an invitation from a supervisor employed by the Board to join a group affiliated with any personal online account of the employee. However, the Board may request or require that an employee provide the Board with a user name and password, password or any other authentication means for accessing (1) any account or service provided by the Board or by virtue of the employee's employment relationship with the Board or that the employee uses for the Board's business purposes, or (2) any electronic communications device supplied or paid for, in whole or in part, by the Board.

In accordance with applicable law, the Board maintains the right to require an employee to allow the Board to access the employee's personal online account, without disclosing the user name and password, password or other authentication means for accessing such personal online account, for the purpose of:

(A) Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee's personal online account; or

(B) Conducting an investigation based on the receipt of specific information about an employee's unauthorized transfer of the Board's proprietary information, confidential information or financial data to or from a personal online account operated by an employee or other source.

For purposes of these Administrative Regulations, "personal online account" means any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including, but not limited to, electronic mail, social media and retail-based Internet web sites. "Personal online account" does not include any account created, maintained, used or accessed by an employee for a business purpose of the Board.

Why Monitor?

The computer systems are expensive for the Board to install, operate and maintain. For that reason alone it is necessary to prevent misuse of the computer systems. However, there are other equally important reasons why the Board intends to monitor the use of these computer systems, reasons that support its efforts to maintain a comfortable and pleasant work environment for all employees.

These computer systems can be used for improper, and even illegal, purposes. Experience by other operators of such computer systems has shown that they can be used for such wrongful purposes as sexual harassment, intimidation of co-workers, threatening of co-workers, breaches of confidentiality, copyright infringement and the like.

Monitoring will also allow the Board to continually reassess the utility of the computer systems, and whenever appropriate, make such changes to the computer systems as it deems fit. Thus, the Board monitoring should serve to increase the value of the system to the district on an ongoing basis.

Privacy Issues

Employees must understand that the Board has reserved the right to conduct monitoring of these computer systems and can do so *despite* the assignment to individual employees of passwords for system security. Any password systems implemented by the district are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user.

The system's security aspects, message delete function and personal passwords can be bypassed for monitoring purposes.

Therefore, *employees must be aware that they should not have any expectation of personal privacy in the use of these computer systems*. This provision applies to any and all uses of the district's computer systems and electronic devices that access same, including any incidental personal use permitted in accordance with these regulations.

Use of the computer system represents an employee's acknowledgement that the employee has read and understands these regulations and any applicable policy in their entirety, including the provisions regarding monitoring and review of computer activity.

Prohibited Uses

Inappropriate use of district computer systems is expressly prohibited, including, but not limited to, the following:

- Sending any form of solicitation not directly related to the business of the Board of Education;
- Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person (such communications *may* also be a *crime*);
- Gaining or seeking to gain unauthorized access to computer systems;
- Downloading or modifying computer software of the district in violation of the district's licensure agreement(s) and/or without authorization from IT Department personnel;
- Damaging equipment through careless handling, loss, or theft;
- Sending any message that breaches the Board's confidentiality requirements, including the confidentiality rights of students;
- Sending any copyrighted material over the system;
- Sending messages for any purpose prohibited by law;
- Storing personal or confidential information on the system;
- Transmission of inappropriate email communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;
- Using computer systems for any purposes, or in any manner, other than those permitted under these regulations;
- Using social networking sites such as Facebook, Twitter, LinkedIn, Instagram and YouTube in a manner that disrupts or undermines the effective operation of the school district, is used to engage in harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate communications; creates a hostile work environment; breaches confidentiality obligations of school district employees, or violates the law, Board policies and/or the other school rules and regulations;
- Violating cybersecurity best practices through the sharing of passwords.

In addition, if a particular behavior or activity is generally prohibited by law and/or Board policy, use of these computer systems for the purpose of carrying out such activity and/or behavior is also prohibited.

Electronic Communications

The Board expects that all employees will comply with all applicable Board policies and standards of professional conduct when engaging in any form of electronic communication, including texting, using the district's computer system, or through the use of any electronic messaging system or electronic device or mobile device owned, leased, or used by the Board. As with any form of communication, the Board expects district personnel to exercise caution and appropriate judgment when using electronic communications with students, colleagues and other individuals in the context of fulfilling an employee's job-related responsibilities, including when engaging in remote teaching or use of a digital teaching platform.

Disciplinary Action

Misuse of these computer systems will not be tolerated and will result in disciplinary action up to and including termination of employment. Because no two situations are identical, the Board or its designee reserves the right to determine the appropriate discipline for any particular set of circumstances.

Complaints of Problems or Misuse

Anyone who is aware of problems with or misuse of these computer systems, or has a question regarding the appropriate use of the computer systems, should report this to a district administrator, supervisor or to the school principal.

Most importantly, the Board urges *any* employee who receives *any* harassing, threatening, intimidating or other improper message through the computer systems to report this immediately. It is the Board's policy that no employee should be required to tolerate such treatment, regardless of the identity of the sender of the message. *Please report these events!*

Implementation

This regulation is effective as of __/__/__.

Legal References:

Conn. Gen. Stat. § 31-40x
Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250

Electronic Communication Privacy Act, 18 U.S.C. §§ 2510 through 2520

[Note: Although we have included this sample notice in our model policy documents for the convenience of our Board of Education clients, the notice does not need to be approved as a Board policy].

NOTICE REGARDING ELECTRONIC MONITORING

[To be posted in a conspicuous place readily available for viewing by employees]

In accordance with the provisions of Connecticut General Statutes Section 31-48d, the Board of Education hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the Board may not actually engage in the use of electronic monitoring, it reserves the right to do so as the Board and/or the Administration deem appropriate in their discretion, consistent with the provisions set forth in this Notice.

"Electronic monitoring," as defined by Connecticut General Statutes Section 31-48d, means the collection of information on the Board's premises concerning employees' activities or communications, by any means other than direct observation of the employees. Electronic monitoring includes the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the Board's premises which are open to the public, or (B) which is prohibited under other state or federal law.

The following specific types of electronic monitoring may be used by the Board in its workplaces:

- Monitoring of electronic messaging systems (including email) and other components of the Board's computer systems, including monitoring of electronic devices such personal computing devices, cellular phones, Smartphones, network access devices, radios, personal cassette players, CD players, tablets, walkie-talkies, personal gaming systems, Bluetooth speakers, personal data assistants, and other electronic signaling devices that access the computer systems, for compliance with the Board's policies and regulations concerning use of such systems.

- Video and/or audio surveillance within school buildings (other than in restrooms, locker rooms, lounges and other areas designed for the health or personal comfort of employees or for the safeguarding of their possessions), on school grounds and on school buses and other vehicles providing transportation to students and/or employees of the school system.

- Monitoring of employee usage of the school district's telephone systems.

- Monitoring of employees when employees are engaging in remote teaching or use of a digital teaching platform.

The law also provides that, where electronic monitoring may produce evidence of misconduct, the Board may use electronic monitoring without any prior notice when the Board has reasonable grounds to believe employees are engaged in conduct that (i) violates the law, (ii) violates the legal rights of the Board or other employees, or (iii) creates a hostile work environment.

Questions about electronic monitoring in the workplace should be directed to the Superintendent.

Legal References:

Connecticut General Statutes:
Section 31-48b
Section 31-48d