4118.35
Personnel

POLICY REGARDING EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Computers, computer networks, electronic devices, Internet access, and e-mail are effective and important technological resources. The Board of Education provides computers, a computer network, including Internet access and an e-mail system, and other electronic devices that access the network such as wireless and/or portable electronic hand-held equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. (including, but not limited to, personal laptops, Smartphones, network access devices, cellular telephones, radios, MP3 and other digital audio players, CD players, tablet computers, walkie-talkies, personal data assistants, digital cameras, and other electronic signaling devices) (referred to collectively as "Computer Systems"), in order to enhance both the educational opportunities for our students and the business operations of the Weston Public Schools ("District").

The Computer Systems are business and educational tools. As such, they are made available to Board employees for business and education related uses. The Administration shall develop regulations setting forth procedures to be used by the Administration in an effort to ensure that such Computer Systems are used for appropriate business and education related purposes.

The system administrator, school and District administrators, and others managing the Computer Systems may access email or monitor activity on the Computer Systems 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 media sites.

Personal use of the Computer Systems is permitted. Such personal use of the Computer Systems, however, is subject to all District policies and regulations, including monitoring of all such use, as well as any rules as the Superintendent may establish. Moreover, any such personal use shall not interfere in any manner with work responsibilities, and all such personal use shall occur outside of designated work periods.

Users should not have any expectation of personal privacy in the use of the Computer Systems or other electronic devices that access the Computer Systems. Use of the Computer Systems represents an employee's acknowledgement that the employee has read and understands this policy and any applicable regulations in their entirety, including the provisions regarding monitoring and review of computer activity.

Legal References:

Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250
Electronic Communication Privacy Act, 28 U.S.C. §§ 2510 through 2520

Policy References:

Policy No. 4118.4, Electronic Mail/Telecommunications
Policy No. 4118.5, Social Networking

ADOPTED: June 17, 2013

R4118.35
Personnel

ADMINISTRATIVE REGULATIONS REGARDING EMPLOYEE USE OF THE DISTRICT'S COMPUTER SYSTEMS AND ELECTRONIC COMMUNICATIONS

Introduction

Computers, computer networks, electronic devices, Internet access, and electronic mail are effective and important technological resources. The Board of Education has installed computers, a computer network, including Internet access and an e-mail system, and may provide electronic devices that access the system, such as personal laptops, Smartphones, tablet computers, personal data assistants, walkie-talkies, or other mobile or handheld electronic devices, to enhance the educational and business operations of the District. In these regulations, the computers, computer network, electronic devices, Internet access, e-mail, and electronic messaging systems are referred to collectively as "Computer Systems."

These Computer Systems are business and educational tools. As such, they are being made available to employees of the District for District-related educational and business purposes. Personal use of the Computer Systems, other than email and electronic messaging systems, is permitted. Such personal use of the Computer Systems, however, is subject to all District policies and regulations, including monitoring of all such use, as well as any rules as the Superintendent may establish. Moreover, any such personal use shall occur outside of designated work periods.

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, some of which are the result of negligence, and others of which are 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.

Unless specifically agreed in writing, all messages, documents, photographs, multimedia, and other digital materials created using the Computer Systems are the property of the Weston Public Schools.

Monitoring

It is important for all users of these Computer Systems to understand that the Board of Education, as the owner or lessee 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 of Education intends to monitor in a limited fashion, but will do so as it deems appropriate 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, school and District administrators, and others managing the Computer Systems may access email or monitor activity on the Computer Systems 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 media sites.

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 shall not be used for improper and/or 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 Computer Systems' 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 Systems 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 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*);

- Using another person's password and/or username to access that person's account or otherwise attempt to gain unauthorized access to the Computer Systems;

- Misrepresenting oneself as another individual or entity and/or modifying files, communications, other data, passwords or usernames belonging to another person and/or to which access is not otherwise available to the employee;

- Leaving a file, email, or other digital document open on any device included in the Computer Systems, when the device is unattended, in a manner that it can be viewed or accessed by another person;

- Gaining or seeking to gain unauthorized access to other "c**o**mputer systems" as that term is defined herein;

- Downloading or modifying computer software of the District in violation of the District's licensure agreement(s) and/or without authorization from supervisory personnel;

- Downloading unauthorized software onto the Computer Systems;

- Sending any message, or otherwise transmitting/publishing information that breaches the Board of Education's confidentiality requirements, including, but not limited to, the confidentiality rights of students;

- Failure to adhere to copyright laws including, but not limited to, using the Computer Systems to reproduce, copy, save, improperly cite, and or distribute materials subject to copyright except as permitted by law;

- Sending messages for any purpose prohibited by law, Board policy, or Administrative Regulations;

- Transmitting, distributing, accessing, storing, or receiving inappropriate e-mail communications, digital media, or documents containing pornographic, vulgar, lewd, obscene, and/or sexually explicit words, pictures, videos, or other digital material;

- Using Computer Systems for any purposes, or in any manner, other than those permitted under these regulations or as specifically directed by the employee's supervisor or the Superintendent;

- Using social media sites in a manner that violates the Board's Social Networking policy (Policy No. 4118.5).

- Physically connecting a device to the Computer Systems with a cable or other non-wireless connection.

It is not the intent of this Policy to exhaustively enumerate all instances of unacceptable use of the Computer Systems. Therefore, if a particular behavior or activity is generally prohibited by law and/or Board of Education 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 Systems, or through the

use of any 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.

All work-related electronic communications shall be conducted via the District's email and electronic messaging systems.

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 reserves the right to determine the appropriate discipline for any particular set of circumstances.

Responsibility for Privately Owned Technological Devices

Employees are responsible for the safety and use of their privately owned technological devices. Employees should be aware that the Board is not liable for any privately owned technological device that is stolen, lost, or damaged while at school or during a school-sponsored activity. In addition, the Board is not liable for damage caused to a privately owned technological device that is infected by a computer virus and/or malware of any kind while it is connected to, or otherwise interacting with, the Computer Systems.

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 his or her supervisor or to the Director of Technology.

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 to the administration.*

The District will take reasonable precautions, as it deems appropriate, to filter objectionable materials (e.g. pornography, drug-related forums, vulgarity, etc.) in order to prohibit Internet access to these materials on the Computer Systems. However, it is not possible for the District to restrict all such materials, and it cannot be held responsible for such materials acquired utilizing the Computer Systems.

Legal References:

Conn. Gen. Stat. § 31-48d
Conn. Gen. Stat. §§ 53a-182; 53a-183; 53a-250
Electronic Communication Privacy Act, 28 U.S.C. §§ 2510 through 2520

Policy References:

Policy No. 1255, Civility
Policy No. 4118.4, Electronic Mail/Telecommunications
Policy No. 4118.5, Social Networking
Policy No. 6184, Unexpected Broadcast

ADOPTED: June 17, 2013