Personnel – Certified / Non-Certified

4118.4(a)

ELECTRONIC MONITORING **4218.4**

In accordance with Connecticut General Statutes, the District hereby gives notice to all its employees of the potential use of electronic monitoring in its workplace. While the District may not actually engage in the use of electronic monitoring, it reserves the right to do so when determined to be appropriate by the Board or the Superintendent of Schools at their discretion.

I. Definitions

A**. "Electronic mail"** is an electronic message transmitted between two or more computers or electronic terminals, whether the message is converted to hard copy after receipt, and whether the message is viewed upon transmission or stored for later retrieval. Electronic mail includes all electronic messages that are transmitted through a local, regional, or global computer network.

B. "Electronic monitoring," as defined by Connecticut General Statutes, means the collection of information on school district 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, photo-electronic, or photo-optical systems. The law does not cover the collection of information (A) for security purposes in any common areas of the District premises which are open to the public, or (B) which is prohibited under other state or federal law.

II. Workplace Electronic Monitoring and Posting Notice

This policy also serves as the required posting notice.

All staff members are made aware of the following:

- Monitoring may be used for assuring compliance with professional codes of conduct, Board Policy, or Administrative Regulations or established practices.
- Virtually, all electronic devices retain a record of each use and the information about that use may be recoverable.
- Electronic communications may not be secure and therefore may not be an appropriate means by which to communicate confidential or sensitive information. Electronic mail and documents sent or received by District employees may constitute public records subject to inspection and disclosure under the Connecticut Freedom of Information Act (FOIA), unless specifically exempted by law.

Personnel – Certified / Non-Certified

4118.4(b)
ELECTRONIC MONITORING (continued) **4218.4**

The following specific types of electronic monitoring may be used by the school district in its facilities:

- Monitoring and auditing of email transmissions, internet browsing, file storage, and network traffic across all District computers, servers, and connected devices.
- Video surveillance in school buildings and on school grounds except where prohibited by law for security purposes.
- Video surveillance on all school transportation vehicles.
- Telephone monitoring (landlines, cell or wireless) for quality control and performance assessment.
- Monitoring of electromagnetic card access system for security purposes.

The law also provides that the District may conduct electronic monitoring without prior written notice when the District and/or Superintendent have reasonable grounds to believe employees are engaged in conduct that (1) violates the law, (2) violates the legal rights of the Board or its employees, or (3) creates a hostile workplace environment, and electronic monitoring may produce evidence of such misconduct.

All computers, servers, software, network infrastructure, email accounts, telephones, and data stored on or transmitted through District systems are the property of the Fairfield Public Schools. Employees should have no expectation of privacy regarding any communications, files, data, or usage associated with district electronic systems or network resources.

The District reserves the right to bypass individual passwords at any time to access system records for maintenance, legal compliance, or investigation. Employees may not share passwords or leave terminals signed on while unattended.

Staff members are expected to conduct themselves professionally and ethically in all electronic communications. Prohibited activities include, but are not limited to:

1. Engaging in illegal activities, gambling, or violating copyright and intellectual property laws.
2. Accessing, sending, or displaying obscene, pornographic, harassing, discriminatory, or offensive content.
3. Transmitting confidential student records or confidential employee details via unencrypted or unauthorized email (pursuant to FERPA and Board Policy).

Personnel – Certified / Non-Certified

4. Utilizing District technology for private commercial gain, personal business ventures, or unauthorized financial commitments.
5. Using District systems to promote, support, or oppose political candidates, ballot measures, or religious institutions.
6. Attempting to bypass network security, sharing passwords, or accessing another employee's account/files without explicit administrative authorization.
7. Disseminating unsolicited mass communications or engaging in activities that degrade system performance or introduce malicious software.

The Superintendent will ensure that all district employees receive notice of this policy and that each employee is provided with an acknowledgment form to sign attesting that they have received and read the policy. The form will be maintained in the employee's personnel file.

Questions about electronic monitoring in the workplace should be directed to the Superintendent of Schools or members of the administrative staff.

Legal Reference: Connecticut General Statutes
The Freedom of Information Act.
31-48d – Employers engaged in electronic monitoring required to give prior notice to employees
Public Act 26-73, An Act Concerning the Electronic Surveillance of Employees

Adopted 8/27/2004
Revised and Adopted 1/29/2013
Revised and Adopted 11/10/2026