PERSONNEL

Workplace Privacy, Monitoring and Internet Use

One of the Coventry Board Of Education's missions is to effectively and efficiently conduct its business and meet or exceed service expectations. In order to do this, the BOARD must be able to: (a) access business information at all times; (b) provide a safe, productive work environment; and (c) supervise its employees to be sure that they are acting consistently with business objectives.

The Coventry Board of Education recognizes the need for computers, electronic communications and internet access systems and the vital role they play in assisting Board employees in delivering exceptional public services. The Board provides computers, electronic communications and internet access systems as tools and it is expected that these tools will be used in an appropriate manner at all times. The primary purpose of computers, electronic communications and internet access systems is to assist in the conduct of business with the school system as a whole. The Board encourages its employees use and proficiency in the operation of electronic communications and internet access, which can improve office efficiencies and the conduct of routine school activities. All information and communication on such systems is the property of the Board of Education, and there is no expectation of privacy.

In order to prevent any misunderstandings, the Coventry Board Of Education believes that every employee should be aware of the following policies on privacy, monitoring and internet use in the workplace so that they can conduct themselves in a professional manner at all times and avoid potentially embarrassing situations.

1. Employees using personal locks on Board property must provide the combination to their supervisor. The Board will also retain a copy and a record of any company keys issued to employees. Employees are personally responsible for lost keys.

2. The Board provides radios, telephones and computers and other forms of electronic communications to employees to facilitate efficient and effective business operations. Electronic communications includes without limitation information that is transmitted, received, and/or stored via the telephone, radios, the voice mail system, the electronic mail (e-mail) system, the facsimile machines and processes, the internet and world wide web, and video systems. These communication systems, as well as all electronic communications transmitted, received, and/or stored on these systems, are subject to review by the Board. As such, employees shall use these communications systems for Board business only, except that incidental personal use of these electronic systems is permitted, involving for instance occasional personal phone calls, e-mails or web access, to the extent that such incidental use does not affect work productivity or job performance, does not cause the BOARD to incur any additional expenses, and does not violate any policies or procedures of the Board or applicable laws.

3. The Board's policy prohibiting harassment and discrimination applies to the use of these systems. Therefore, the creation, transmission, receipt or downloading of inappropriate or offensive comments or other images or information, such as disparaging comments or pictures based on race, ethnicity, religion, age, gender, national origin, disability, sexual orientation or any other protected category, over any of the Board's systems is prohibited.

4. The Board's electronic communications systems may not be used to solicit for religious or political causes, outside organizations or other personal matters unrelated to employment with the Board.

5. World Wide Web access and use of the Internet is encouraged where such use is appropriate for business and professional objectives and is conducted lawfully.

6. Messages communicated over the Board's electronic communications systems must not be transmitted under an assumed name, and users may not attempt to obscure the origin of any message. Finally, care should be taken in the transmission of confidential information involving the Board's operations being sent or received via the internet.

7. Software and approved programs and materials, other than those that have been properly licensed by the Board, may not be installed or downloaded on the Board's computers without prior permission. In addition, theft of software is a crime, and is punishable by law. Users are not permitted to copy, transfer, rename, add or delete information on programs belonging or licensed to others unless given express permission to do so. No employee may use the Board's electronic communications systems in ways that are inconsistent with licenses or copyrights, or to download or distributed pirated software or data. Furthermore, no employee may use the Board's electronic communications systems to propagate any virus, worm or trap door program code, or to otherwise disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

8. Intrusions of another employee's privacy will not be tolerated. The tape recording of any conversation in the workplace is strictly prohibited without written authorization from the Superintendent of Schools or with the consent of all parties to the conversation. The tape recording of any telephone conversation to or from the workplace is strictly prohibited absent the consent of the parties to the phone call obtained in accordance with applicable law. The sole exceptions are the emergency dispatch lines at the Police Department that are taped at all times (742-7331, 742-4071, 742-4072).

9. The Board reserves the right to review, access, and intercept all messages created, perceived, or sent over its electronic communications system at any time, without advance notice, this shall not apply to private employee organization communication, for such reasons as, without limitation: ensuring that the systems are primarily being used to conduct the Board's business; maintaining the system; preventing or investigating allegations of system abuse or misuse; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; and ensuring that the Board's operations continue appropriately. An employee's use of the Board's communications systems constitutes consent to the Board's conduct. This policy constitutes notification subject to Public Act No. 98-142.

10. Employees are prohibited from gaining access to another employee's computer or other electronic communications and must not use unauthorized codes, passwords or other means to gain access to another employee's computer or other electronic communications systems, unless expressly permitted to do so by authorized management personnel. Employees are prohibited from accessing a file or retrieving any stored information on the Board's e-mail, voice-mail, and computer systems unless expressly permitted to do so by authorized management personnel or in cases where the material was originated by the employee making the request. Employees should not create their own computer, voice-mail or other electronic communications system passwords unless permitted to do so by authorized management personnel. Employees must provide all personal passwords to the Board so that the Board may effectively conduct business at all times.

11. Public records retention and Freedom of Information requirements must be satisfied in the use of electronic communications systems in accordance with the Board's policies and applicable law. A copy of the Schedule of Retention of Records is available in the Office of the Superintendent of Schools.

12. Any employee who violates the Board's privacy, monitoring and internet use policy shall be subject to disciplinary action, up to and including termination of employment. In addition, criminal penalties and fines may apply where the employee's conduct violates applicable state or federal laws.

13. Any complaints regarding potential violations of this policy, and/or any questions regarding an employee's use of these electronic communication systems in accordance with this policy, should be directed to the Superintendent of Schools.

For more information regarding technology security, please see the Coventry Public Schools' Disaster Recovery Plan. This procedure is available through the Coventry Superintendent of Schools.

First adopted: October 25, 2001

Revised: June 8, 2006

Revised: January 8, 2009