Personnel – Certified/Non-Certified

Policy regarding Employee Use of the District's Computing Systems

District computing devices, networks, Internet access, and electronic communications are effective and important technological resources in today's educational environment. The Board of Education has installed computing devices, networks, including Internet access and electronic communications (referred to collectively as "the computing systems"), in order to enhance both the educational opportunities for our students and the business operations of the district.

These computing 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. *All users of the computing systems must restrict themselves to appropriate district-related educational and business purposes*. Incidental personal use of the computing systems may be permitted solely for the purpose of electronic communications and access to the Internet on a limited, occasional basis. Such incidental personal use of the computing systems is subject to all rules, including monitoring of all such use, set out in this policy. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities.

Monitoring

It is important for all users of these computing systems to understand that the Board of Education, as the owner of the computing systems, reserves the right to monitor the use of the computing systems to ensure that they are being used in accordance with this policy. The Board of Education 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 computing systems by any or all employees at any time.

Why Monitor?

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

While computing devices can be used for improper, and even illegal, purposes, it is prohibited to do so. Experience by other operators of such computing 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 computing systems, and whenever appropriate, make such changes to the computing 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 computing 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 computing systems*. This provision applies to any and all uses of the district's computing systems, including any incidental personal use permitted in accordance with this policy.

Prohibited Uses.

Inappropriate use of district computing 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 supervisory personnel;
- Sending any message that breaches the Board of Education's confidentiality requirements, including the confidentiality rights of students;

- Distributing any copyrighted material over the system;
- Sending messages for any purpose prohibited by law;
- Transmission or receipt of inappropriate electronic communications or accessing inappropriate information on the Internet, including vulgar, lewd or obscene words or pictures;
- Using computing systems for any purposes, or in any manner, other than those permitted under these regulations.

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

Disciplinary Action.

Misuse of these computing systems will not be tolerated and will result in disciplinary action up to and including termination of employment. As no two situations are identical, the Board 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 computing systems, or has a question regarding the appropriate use of the computing systems, should report this to his or her supervisor, to the Business Administrator, or to Tech Repair.

Most importantly, the Board urges *any* employee who receives *any* harassing, threatening, intimidating or other improper message through the computing 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.

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

NORWICH PUBLIC SCHOOLS
Norwich, Connecticut

Policy Approved: 6/19/07
Policy Revised: 6/9/15