Series 4000 – Personnel – Certified & Non-Certified

1. Certified Personnel

A. Permanent Personnel

(8) Rights, Responsibilities and Duties

(e) Computers: Responsible Use Agreement of the Internet, Other Computer Networks and Internet Safety

While using District provided and personal technology resources, each employee must act in an appropriate manner consistent with ethical and legal principles as well as the District's expectations outlined herein. This includes any remote access which employees may gain off-site, but which involves the use of District sites, servers, intranet facilities, email accounts, software, or equipment. It also includes the use of personal technology resources when such personal resources are utilizing District servers, intranet facilities, email accounts, software, or storing or accessing District data.

Scope of Policy

In the interest of providing new and emerging educational benefits for communication and data management technologies, and for classroom instructional technologies, it is the policy of the Suffield Public Schools (the "District") to afford broad access to District computers, communications systems, the Internet, and an array of technology resources for District employees to use in fulfilling the District's mission. The purpose of this Employee Responsible Use Policy is to outline what is responsible use by employees of District technology resources and personal technology resources that access or use District resources. The principles outlined herein are in place to protect both the employee and the District. This policy applies to all non-student users of the District's provided and personal technology resources. (Student users of the District provided and personal technology resources are governed by a separate Responsible Use Policy.) It is the sole responsibility of each employee to be informed about his/her responsibilities and the District's expectations for the responsible use of District provided and personal technology resources.

Definitions

District Technology Resources:

For the purposes of the District's Employee Responsible Use Policy ("RUP"), "District Technology Resources" refers to the District's computers; District issued personal data devices (including Smartphones, Blackberries, PDAs, other mobile or handheld devices) and instructional technologies; communications and data management systems; informational technologies and the Internet; and a variety of other technology resources in order to promote educational excellence.

Employee:

For the purposes the District's RUP, the term "employee" shall be deemed to include contractors, volunteers, Board of Education members, third parties and other non-student members of the school community including substitutes and temporary employees.

Personal Technology:

For the purposes of the District's RUP, "personal technology" refers to privately owned wireless and/or portable equipment that can be used for word processing, wireless Internet access, image capture and recording, sound recording, information transmitting and/or receiving, storing, etc. These devices may include, but are not limited to, personal laptops, Smartphones, network access devices, and other electronic signaling devices.

Privacy Issues and Incidental Personal Use

Access to District provided and personal technology resources carries with it the responsibility for ensuring that the use of these resources is primarily for District purposes and District-related activities, and for maintaining the integrity and security of the District's technology equipment and facilities. The District provided and personal technology resources have not been established as a public access service or as a public forum. The District has the right to place reasonable restrictions on the material employees access or post through the District provided and personal technology resources. Employees must understand that the Board has reserved the right to conduct monitoring of these District provided and personal technology resources 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 District provided and personal technology resource user. The District provided and personal technology resources' 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 technology resources. This provision applies to any and all uses of the District provided and personal technology resources and District electronic devices and personal technology used to access same, including any incidental personal use permitted in accordance with this policy and any applicable regulations. Use of the District provided and personal technology resources represent 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 activity involving the District provided and personal technology resources.

In the interest of making the use of District provided and personal technology resources a natural part of the day-to-day work of all members of the District community, incidental personal use is acceptable. Incidental personal use of the District provided and personal technology resources is permitted solely for the purpose of e-mail transmissions and access to the Internet on a limited, occasional basis. Such incidental personal use of the District provided and personal technology resources, however, is subject to all rules, including monitoring of all such use, as the Superintendent may establish through regulation. Moreover, any such incidental personal use shall not interfere in any manner with work responsibilities, and the use of District provided and personal technology resources is prohibited for personal purposes during assigned work time. Use of District provided and personal technology resources for personal purposes should be

incidental, done on the employee's own time, and at the employee's own risk. The District provided and personal technology resources shall never be used to solicit commercial sales for personal benefit or for political lobbying. Employees must recognize that personal information stored or passed through the District provided and personal technology resources may be subject to the Freedom of Information Act or other state or federal laws governing the disclosure of information.

Effective security of District provided and personal technology resources is a team effort that involves the participation and support of every employee. Employees must respect the integrity and security of the District's technology resources systems, and the access privileges, privacy, and reasonable preferences of other users. Employees having access to District provided and personal technology resources must take reasonable care to ensure that unauthorized persons are not able to use their access to the District provided and personal technology resources. The use of the District provided and personal technology resources may involve the use of a password, network access code, or other identifying or validating code. Such passwords and codes must be protected as private information provided to the individual user for their sole use. Such passwords and codes shall not be disclosed by the employee to others. Employees shall immediately notify the Information Technology (IT) Department if they have identified possible security problems related to the District provided and personal technology resources. Employees further agree to avoid the inadvertent spread of computer viruses by following the District's virus protection procedures.

The District provided and personal technology resources are, by nature, finite. Employees must recognize that certain uses of the District provided and personal technology resources may be limited for reasons related to the capacity or security of the District provided and personal technology resources, or as required for fulfilling the District's primary instructional mission.

No information technology resources can absolutely guarantee the privacy or confidentiality of electronic data, information, or the transmission of such. However, all employees shall take reasonable precautions to protect electronic data, information and the transmission of such containing private and confidential information. The privacy and protection of personally identifiable student and employee data is of paramount importance. Likewise, the safeguarding of physical technology resources assigned to employees is the responsibility of the employee. It is the employee's responsibility to report the loss of private and confidential information, and the loss of technology equipment to the District's Information Technology Department immediately upon discovery of the loss.

Applicable Standards for Use of District Provided and Personal Technology Resources

In addition to the general principles set forth in this Employee Responsible Use Policy, the use of District provided and personal technology resources may be affected by a number of other legal and ethical principles. While it is not possible to list all potentially applicable laws, regulations, and local standards, the following are provided:

1. The use of District provided and personal technology resources may involve the use of a password, network access code, or other identifying or validating code. Such passwords and codes are to be protected as private information provided to the individual user for their sole purpose and use. Such passwords and codes shall not be disclosed by the employee to others.

2. District provided and personal technology resources shall not be used for any activity, or to transmit any material, that violates federal, state, or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright or other intellectual property laws, and any threat or act of intimidation or harassment against another person. The District provided and personal technology resources users may not intentionally create, store, display, print, or transmit information which violates the District's Sexual Harassment Policy.

3. District provided and personal technology resources shall not be used to download, copy, or store any copyrighted software, publications, music, video, or other content without permission from the copyright holder. Any software that is installed on the District provided and personal technology resources shall be properly licensed from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s). The District retains the right to remove software or language from websites that are not compliant with copyright laws or applicable license(s), or that cause the workstation to become unstable or consume excessive technology resources.

4. The use of District provided and personal technology resources is not private; employees should not expect that files stored on or transmitted via the District's provided and personal resources will be confidential. All digital transmissions are subject to inspection and/or monitoring by District employees and other officials. Digital storage is the District's property, and as such, network administrators will review files and communications to maintain system integrity and ensure that employees are using technology responsibly. Data, information, and transmissions using District provided and personal technology resources constitute public records and are subject to public records retention and release laws.

5. Employees are expected to model excellent communication skills, sound judgment, and good manners at all times while using District provided and personal technology resources. District provided and personal technology resources users agree not to send, access, submit, publish, display or print hate mail, defamatory statements, vulgar, derogatory, obscene, profane, sexually oriented, threatening, offensive or illegal material or language over the Internet or the District provided and personal technology resources. District provided and personal technology resources users shall not access Web sites, newsgroups, or chat areas that contain material that is prohibited under child pornography laws or that promotes any illegal act. The use of District provided and personal technology resources in a manner intended to injure or humiliate others by disclosure of personal information (whether true or false), by personal attacks on others, by disparaging or angry statements expressed toward any person, or by disparagement of any person's or group's race, color, religion, national origin, gender, sexual orientation, or disability are strictly prohibited. Cyberbullying is specifically prohibited. It shall be the employee's responsibility to immediately report any inappropriate use, web site, or communication to the employee's supervisor.

6. District provided and personal technology resources users shall not post anonymous messages or attempt to impersonate another person by forging email, web pages, or other electronic media.

7. District provided and personal technology resources users may not log onto another user's account, IP address, or other resource access, or attempt to access another user's

files, or permit anyone else to log onto their own accounts. Users may not try to gain unauthorized access ("hacking") to the files or technology systems of any other person or organization.

8. The primary use of the District provided and personal technology resources is for District-related work. While some incidental personal use of the District provided and personal technology resources is permitted as discussed above, such incidental personal use will not be deemed a waiver of the District's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis.

9. District provided and personal technology resources users shall not use District provided and personal technology resources to conduct business activities or to engage in political activities. Employees shall not use District provided and personal technology resources for advertising, promotion or commercial purposes, or similar objectives.

10. District provided and personal technology resources users shall not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material ("spamming"). District provided and personal technology resources users shall not create or forward "chain letters", "Ponzi schemes", or other "pyramid" schemes of any type.

11. Virtual and physical vandalism of District provided and personal resources shall not be tolerated. Any intentional act by an employee that damages or interferes with performance of District provided and personal technology hardware, software, operating systems, data management systems, or communication systems will be considered vandalism and the employee will be subject to discipline and/or appropriate criminal or civil action. The District provided and personal technology resources users shall not introduce malicious programs into the District provided and personal technology resources (e.g. malware, viruses, worms, Trojan horses, email bombs, etc.). District provided and personal technology resources users shall not intentionally disrupt network traffic or crash the network and connected systems; users shall not degrade or disrupt equipment or system performance.

12. Employees may bring personal technology, including computers, Smartphones, network access devices, or other electronic signaling devices to their work place. However, the District is not responsible for the safeguarding of such personal technology. Employees must abide by the protocols outlined in the Bring Your Own Technology (BYOT) policy and the following:

    - The District's network filters will be applied to an employee or student connection to the Internet, and no attempt will be made to bypass these filers.
    - Knowingly bringing on school grounds and/or infecting the network with a virus, malware, or other program designed to damage, alter, destroy, or provide access to unauthorized data or information is prohibited.
    - Processing and accessing information on school property related to "hacking", altering, or bypassing network security policies is prohibited.
    - The District has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.

13. Employees shall not take data, equipment, software, or supplies for their own personal use. Such behavior will be treated as theft. Employees may take computer equipment home or to off-site destinations for District-related purposes.

The District will cooperate fully with local, state and federal officials in any investigation related to any suspected illegal activities conducted through District provided and personal technology resources. Employees who violate this Employee Responsible Use Policy are subject to disciplinary action, up to and including termination of employment. As no two situations are identical, the District reserves the right to determine the appropriate discipline for any particular set of circumstances.

All employees and contracted service providers shall sign a "User-Responsibility Acknowledgement" acknowledging their receipt and understanding of the Employee Responsible Use Policy and its related protocols and regulations.

(cf. 6141.321 – Student Responsible Use Policy for Use of District provided and personal Technology Resources)

Legal References: Connecticut General Statutes

The Freedom of Information Act

53A-182B Harassment in the first degree

P.A. 98-142 An Act Requiring Notice to Employees of Electronic Monitoring by Employers

Regulation adopted: September 7, 2000
Policy revised: May, 22, 2006, June 28, 2011
August 21, 2012, June 3, 2014

SUFFIELD PUBLIC SCHOOLS
Suffield, Connecticut

4118.5
4218.5
FORM

Personal – Certified/Non-Certified

Rights, Responsibilities and Duties

Suffield Public Schools
Employee Responsible Use of District Provided and Personal Technology Resources
User Responsibility Acknowledgement

I have received the Employee Responsible Use Policy for Use of District provided and personal Technology Resources. I have read, understand, and acknowledge that I am required to abide by the Suffield Public Schools District's policies and administrative regulations for the use of technology resources, including the "Bring Your Own Technology" policy and any applicable regulations. I further understand that any violation of these policies or administrative regulations for the use of technology resources is unethical and may constitute a criminal offense. I acknowledge that, should I commit any violation, disciplinary action and/or other appropriate legal action may be taken.

Employee Name (please print): _____

Employee Signature: _____ Date: _____