

## ACCEPTABLE EMPLOYEE USE AND INTERNET SAFETY POLICY

The Schodack Central School District (the “District”) is pleased to provide access to computerized information resources through the District’s Computer Network (DCN), consisting of software, hardware, computer networks and electronic communication systems. All employee use of the DCN shall be subject to this Policy.

In order for the District to be able to continue to make its DCN and Internet access available, employees must take responsibility for appropriate and lawful use of this access.

### I. Acceptable Uses

A. **Educational Purposes Only.** The District is providing employee access to its DCN and the Internet for educational purposes only. If an employee has any doubt about whether a contemplated activity is educational, he or she may consult with a supervisor to determine if a use is appropriate.

### B. **Unacceptable Uses of Network**

- 1) Uses that violate the law or encourage others to violate the law. Employees may not engage in any use which is in violation of the law, or encourage others to do so, including but not limited to the following activities: transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the District’s policies and/or applicable law; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; or download or transmit confidential trade secret information, or copyrighted materials. Even if materials are not marked with the copyright symbol, employees should assume that all materials are protected unless explicit permission is given to use them.
- 2) Uses that cause harm to others or damage to their property. For example, employees may not engage in defamation (harming another’s reputation by lies); employ another’s password or some other user identifier that misleads message recipients into believing that someone other than the actual user is communicating or otherwise using his/her access to the network or the Internet. Employees may not upload a worm, virus, “Trojan horse,” “time bomb” or other harmful form of programming, participate in “hacking” activities or any form of unauthorized access to other computers, networks, or information systems.
- 3) Uses that jeopardize the security of access and of the computer network or other networks on the Internet. For example, employees may not disclose or share their password with others or impersonate another person.
- 4) Uses that are commercial transactions. Employees may not sell or buy anything over the Internet. Employees should not give others private information about themselves or others, including credit card numbers and social security numbers.

5) Uses that may damage the DCN. Employees may not use or install unauthorized software on the DCN or change, copy, rename, delete or otherwise access files not created by another without the express permission from the owner/creator of the file. Physical vandalism to the DCN, computers and software (e.g., prying keys off keyboards, inserting foreign objects into disk drives) is also strictly prohibited.

C. **Etiquette.** All DCN users are reminded that access to the DCN and Internet is for educational purposes. As representatives of the school community, employees are encouraged to be mindful of rules of network etiquette, including:

1) Forwarding and Redistributing Messages. Employees should not assume that a sender of e-mail is giving his or her permission to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when employee

2) Sending Attachments. Employees should be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

## II. INTERNET SAFETY

A. **“Hacking” and Other Illegal Activities.** It is a violation of this Policy to use the DCN or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

B. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the written permission of a parent or guardian or, if the student is 18 or over, the written permission of the student himself/herself.

C. **Active Restriction Measures.** The District will utilize filtering software or other technologies in an effort to prevent DCN users from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The District also will monitor the online activities of employees through direct observation and/or technological means, to ensure that employees are not accessing such depictions or any other material or sites which are unauthorized by this policy.

Internet filtering software or other technology-based protection systems may be disabled by a supervisor or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students.

D. **User Password Policy.** All DCN users are required to change their password at least four times per year. The password must meet the following criteria:

- 1) Must be at least eight characters long.
- 2) Must contain three of the following four categories: capital letter, small letter, number, special character.
- 3) Must not have been used during the previous six passwords (no recycling of passwords).

### III. **PRIVACY**

The DCN and Internet access is provided as a tool for students' education and employee convenience. The District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the DCN and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the District, and no employee shall have any expectation of privacy regarding such materials.

### IV. **FAILURE TO FOLLOW POLICY**

The use of the DCN and Internet is a privilege, not a right. An employee who violates this Policy may, at a minimum, have his or her access to the computer network and Internet withdrawn and may be subject to disciplinary action. An employee violates this Policy if he or she permits another to use his or her account or password to access the DCN and Internet, including any student or employee whose access has been denied or terminated. The District reserves the right to pursue legal action against an employee who willfully, maliciously or unlawfully damages or destroys property of the District or who subjects the District to legal liability through their use of the DCN or Internet.

### V. **WARRANTIES/INDEMNIFICATION**

The District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of the DCN and the Internet provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any employee arising out of the uses of the DCN or the Internet under this Policy. Upon use of the DCN or the Internet, employees are deemed to have agreed to indemnify and hold the District and its administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from their access to the DCN and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services.

Approved: March 18, 2010 (1<sup>st</sup> 1/21/10; 2<sup>nd</sup> 2/25/10; 3/18/10)