No. 524

CATASAUQUA AREA SCHOOL DISTRICT

SECTION: **Classified Employees**

TITLE: **Acceptable Computer Use / Internet Safety Policy**

ADOPTED: **June 11, 2003**
REVISED: **November 10, 2005**
REVISED: **June 10, 2009**
REVISED: **February 13, 2012**

Catasauqua Area School District Acceptable Computer Use / Internet Safety Policy

Section I. Responsibilities and Privileges

a. Purpose and Goals of District Provision of Internet Access

The Catasauqua Area School District (CASD) will provide access to the district network and Internet for students with their parent's or guardian's consent to locate material to meet their educational and personal information needs. School library media specialists and teachers will work together to help students develop the critical thinking skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet educational goals that are consistent with the school district's strategic plan and standards.

CASD will also provide access to the district network and Internet for employees in order to fulfill the requirements of their position(s) as well as an information resource.

Access to the district network and Internet through school resources is a privilege, not a right, and may be revoked for anyone who uses these resources inappropriately as determined by school district authorities.

Catasauqua Area School District Acceptable Computer Use / Internet Safety Policy — Page 2

b. Inappropriate Materials Warning

Due to the nature of the Internet as a global network connecting millions of computers around the world, inappropriate materials, including pornography and obscenity, may be accessed through the Internet connected district network. While appropriate technological filtering mechanisms have been put in place to control access to content classified as obscene, pornographic or harmful to minors, CASD cannot completely block access to these resources because of the nature of the technology that allows the Internet to operate. Accessing these and similar types of resources through the school district network or transmitting such resources to school district networks from another site will be considered an unacceptable use of school district resources and will result in suspension of network, Internet, and computer privileges and other disciplinary action as outlined in appropriate district policies, included in building handbooks and on the CASD website, up to and including suspension and expulsion of students and termination of employees.

c. Education

The school district will ensure that all grade levels will receive age appropriate instruction on matters of safe Internet conduct, including cyberbullying awareness and response and proper interacting on social networking sites and chat rooms.

The school district will further inform all users regarding their individual responsibility to refrain from engaging in unacceptable uses of the network and as to the consequences of their actions if they do so.

d. Monitoring

In an effort to maintain a safe computing environment, district staff will monitor the online activities of students to the extent feasible. Such monitoring may include both direct examination of computers by teachers and other employees as well as remote technological monitoring tools. District staff may also monitor the online activities of employees through direct and remote means.

e. Technology Protection Measures

District Administration shall implement and maintain a technology protection measure that blocks or filters Internet access from any school computer or the school district network to protect against access to visual depictions that are obscene, child pornography, or harmful to minors, and any other inappropriate matter or materials harmful to minors. Adult employees shall be afforded a means to access appropriate Internet sites which are otherwise blocked or filtered by the technology protection measure, upon request to the Technology Department. Instructional employees and District administrators are authorized to permit student users to view appropriate Internet sites which are otherwise blocked or filtered by the technology protection measure, upon request to the Technology Department, so long as the employee or administrator personally and directly monitors the student's use of otherwise blocked or filtered sites to protect against access to visual depictions that are obscene, child pornography, or harmful to minors, and so long as the employee or administrator insures that the blocking/filtering technology protection measure is reactivated before the end of the direct monitoring.

f. Authentication Security

To ensure security of sensitive network based data (on internal data / messaging servers as well as the Student Information System), user login credentials for all employees and external authorized users will be subject to enforced requirements on passwords and related syntax. Passwords will have a life limited to 30 days, minimum expected complexity, and restrictions on reusing from recent history. The systems will also lockout users after 3 unsuccessful login attempts. Students may be subject to a lower level of authentication security at the discretion of the District. It is expected that all network users will comply with and not seek to circumvent these security provisions.

g. Definitions

When used in this policy—

1. the term "user" includes both students and employees who are provided access to the district network and Internet through school resources;

2. the term "obscene" shall have the same meaning as defined for that term in 18 U.S.C. § 1460;

3. the term "child pornography" shall have the same meaning as defined for that term in 18 U.S.C. § 2256;

4. the terms "sexual act" and "sexual contact" shall have the same meanings as defined for such terms in 18 U.S.C. § 2246;

5. the term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that—

   (A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
   (B) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   (C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Section II. Authority

The Catasauqua Area School District reserves the right to determine which computer and network services will be provided through school district resources. It reserves the right to view and monitor all applications provided through the network, to log Internet use by users, review e-mail, and to monitor file server space utilization by users, and the information contained therein shall remain the property of the District and may be used as the District sees fit, including serving as the basis for disciplinary action and referral to outside authorities. Users acknowledge NO expectation of privacy in their use of the district network and computers. The school district reserves the right to revoke user privileges, remove user accounts, and refer to legal authorities when violations of this and any other applicable district policies, including those governing network use, e-mail, copyright, security, and vandalism of district resources and equipment occurs. The District makes no warranties of any kind, whether expressed or implied, for the service it is providing, and will not be responsible for any damages a user suffers. This includes, without limitation, loss of, damage to, or unavailability of data or other information, whether caused by the District's own negligence, a user's errors or omissions, or otherwise. Use of any information obtained via the Internet or the District network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through the Internet's services. E-mail may only be made available to students or other minors if the District provides for the safety and security of minors when using e-mail, such as by the use of the Gaggle system to filter potentially inappropriate e-mails to or from student accounts and to notify District administrators of such filtered e-mails. The District will not be held liable for the receipt and/or transmission of inappropriate content.

Catasauqua Area School District Acceptable Computer Use / Internet Safety Policy — Page 5

Section III. Procedures

Network accounts may be used only by the authorized user of the account for its authorized purpose. Accounts will be made available according to a schedule developed by appropriate district authorities given the capability of district hardware. Accounts will be given out to only those individuals who meet the following requirements, and individuals without a network account (*e.g.*, certain elementary school students) may be given access to school computers, the district network, or the Internet only if such persons meet the following requirements:

1. Have read the District Acceptable Computer Use/Internet Safety Policy and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate district authority. Student users must also have their parent or guardian sign this signature page indicating the parent or guardian's agreement with the policy and their consent to allow the student to access and use the network.

2. Have participated in a district orientation which will include but not be limited to network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities.

Section IV. Prohibitions

The use of the District Network, Internet, or any school computers for illegal, inappropriate, unacceptable, or unethical purposes is prohibited. The activities listed below are strictly prohibited by all users of the district network and school computers. The Catasauqua Area School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network. These prohibitions are in effect any time school district resources are accessed in any way, whether in school or at another location, and whether connected directly to the school district network or computers or indirectly through another Internet service provider.

- Allowing another person to use an assigned account or password.

- Use of the network to transmit material likely to be offensive or objectionable to recipients.

- Use of the network to participate in inappropriate and/or objectionable news groups.

- Use of the network to transmit hate mail, harassment, discriminatory remarks, and other antisocial communications on the network.

- Use of the network to order or purchase in the name of the school district or in the name of any individual any type of merchandise or service, unless expressly authorized to do so as part of the user's employment duties. All costs to the district or any individual incurred because of this type of violation will be the responsibility of the user.

- Use of the network to subscribe to any fee-based on-line/Internet service, unless expressly authorized to do so as part of the user's employment duties. All costs to the district or any individual incurred because of this type of violation or any other unauthorized charges or fees resulting from access to the network or the Internet will be the responsibility of the user.

- Use of the network or school computers which results in any copyright violation.

- The unauthorized installation, distribution, reproduction or use of software on district computers or servers. Software may only be installed on district servers by the Technology Department. Software may only be installed on district computers when expressly authorized by the Technology Department.

- Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users, or to misrepresent other users on the network.

- Use of school technology or the network for fraudulent copying, communications, or modification of materials in violation of local, state, or federal laws.

- Destruction, modification, abuse, or unauthorized access to district computer hardware, software, or files including: loading, downloading, or use of unauthorized games, programs, files or other electronic media.

- Destruction of district computer hardware or software.

- Use of the network to participate in unauthorized Internet Relay chats or web based chat rooms (on-line real-time conversations).

- Use of the network to facilitate unauthorized access, including all forms of "hacking", or any other illegal or unlawful activity.

- Use of the network for the unauthorized disclosure, use, or dissemination of personal identification information or other personal or confidential information of others.

- Use of the network by any employee for instant messaging unless expressly authorized as part of the user's employment duties.

- Use of the network by any student for instant messaging unless such use is either (1) expressly authorized by an administrator and directly monitored by an administrator or instructional employee, or (2) provided for under a student's Individualized Education Program or Rehabilitation Act Section 504 Plan and directly or indirectly monitored by an instructional employee. The term "indirect monitoring" includes intermittent direct monitoring coupled with periodic review of usage logs to insure appropriate usage.

- Use of the network by a student for accessing non-school e-mail accounts.

- Use of the network for commercial or for-profit purposes.

- Use of equipment in any manner that would disrupt network use by others.

- Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.

- Use of the network to access or process pornographic or similar material.

- Use of the network by a minor to access visual depictions that are obscene, child pornography, or harmful to minors.

- Use of the network by an adult to access visual depictions that are obscene, child pornography, or harmful to minors unless necessary as part of the user's employment duties and no minors have access to the room in which the visual depictions are viewed.

- Use of a computer that has been logged in under another user's name, except where expressly authorized by the Technology Department for young students without network accounts, or other use of the network account or password of another user.

Section V. Consequences of Abuse of Responsibilities and Privileges

Any user of the network, who violates the prohibitions listed in Section IV of this policy, engages in any other act determined to be an unacceptable use of the network by school authorities, or violates any other district policy governing use of school resources or copyright law, will have his or her user privileges revoked and may face other disciplinary procedures, up to and including suspension and expulsion of students and termination of employees. In addition, illegal use of the network, intentional deletion or damage to files of data, destruction of hardware, copyright violations, or any other activity involving the violation of local, state, or federal laws will be reported to the appropriate legal authorities for prosecution.

		48