No. 824

SECTION: **Operations**

CATASAUQUA AREA SCHOOL DISTRICT

TITLE: **Acceptable Use of Technology Resources, Electronic Communications, and Information Systems**

ADOPTED: **June 11, 2003**
REVISED: **November 10, 2005**
REVISED: **February 13, 2012**
REVISED: **February 20, 2024**
REVISED: **August 13, 2024**

824 – ACCEPTABLE USE OF TECHNOLOGY RESOURCES, ELECTRONIC COMMUNICATIONS, AND INFORMATION SYSTEMS

1. Responsibilities and Privileges

A. Purpose and Goals of District Provision of Internet Access

The Catasauqua Area School District (CASD) will provide access to technology resources (including but not limited to electronic communications systems, computers, tablets, smartphones, computer networks, servers, networked devices, hardware, software, internet access, social media accounts, mobile devices, peripherals, calculators, scanners, printers, portable hard drives, copiers, projectors, televisions, video and sound systems, and cameras) for students with their parent's or guardian's consent to locate material to meet their educational and personal information needs. The Instructional Technology Coordinator, Curriculum Director, 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 may also provide access to district technology resources for employees in order to fulfill the requirements of their position(s) as well as an information resource, and to authorized guests.

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

The District may also provide public access to District-owned social media accounts as a dedicated public forum for communications.

The School Board supports the use of the District's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the District,, and to carry out legitimate business and operation of the District. The District provides these resources for educational and operational purposes, and not as a public access service or to provide a public forum.

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. All online activity, as well as any files stored on District technology resources, may be inspected at any time for any reason by authorized District

personnel. The District may decrypt and inspect encrypted internet traffic and communications to ensure compliance with this policy.

E. Technology Protection Measures and CIPA Compliance

Children's Internet Protection Act, 47 USC § 254; 34 CFR § 54.520; Pa. Child Internet Protection Act, 24 PA. STAT. ANN. § 4601 *et seq.*

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 are subject to district user authentication security measures. Students may be subject to a lower level of authorization security at the discretion of the District. It is expected that all network users will comply with and not seek to circumvent these security measures.

G. Use of Personal Electronic Devices

The use of personal electronic devices on the District network is permitted only on designated networks. When a user connects a personal electronic device to a District network or technology resource, this policy shall apply. Users are subject to the same levels of monitoring and access as if a District-owned device were being utilized. Users who connect a personal electronic device to a District network explicitly waive any expectations of privacy in the content exchanged over the District technology resources.

2. Definitions

When used in this policy—

A. "User" includes students, employees, and guests who are provided access to district technology resources;

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

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

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

E. "Harmful to minors" means any picture, image, graphic image file, or other visual depiction that—

1. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. 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

3. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

F. "Social media" shall mean a category of Internet-based resources that integrate user-generated content and user participation to share information, ideas, personal messages and other content, including photos and videos. Social media includes social networks, which are online platforms where users can create profiles, share information and personal messages, and connect with others.

G. "District-owned social media account" shall mean a social media account, regardless of platform, that is approved by the Board and operated by a designated District employee(s), and is designed to further the educational mission of the District by providing information to the school community and general public.

H. "Personal social media account" shall mean a social media account, regardless of platform, that is attributed to and operated by an employee, individual school director, or student for personal use and is not approved by the Board as an official communications channel of the District.

I. "Designated public forum" is created when a District-owned social media account is intentionally opened for use by the public as a place for expressive activity where members of the public may communicate, post or comment on information, subject to viewpoint neutral rules designated by the Board. In terms of social media, this would include the ability of public users to comment on or reply to social media posts, pictures, or videos.

3. Authority and Delegation of Responsibility

The Catasauqua Area School District reserves the right to determine which technology resources will be provided by the District. 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. 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 district technology resources, whether on or off District property.** 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 Board designates the Superintendent or designee to oversee all District-owned social media accounts and serve as the primary contact person for District-owned social media accounts.

The Superintendent or designee shall notify students and staff about this policy through posting on the District website and by other appropriate communication methods.

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 an e-mail content monitoring system. The District will not be held liable for the receipt and/or transmission of inappropriate content.

4. 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:

A. Have read the District Acceptable Use of Technology Resources, Electronic Communications and Information Systems 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.

B. 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.

5. District-owned Social Media Accounts

A. In General.

The Superintendent or designee shall approve all official social media accounts created and/or maintained as District-owned accounts, including social media accounts for individual schools within the District.

All District-owned social media accounts shall display the official name and logo and/or mascot of the District or a school.

The Superintendent or designee shall establish which District-owned social media accounts may operate as a designated public forum, where the public may comment and interact with information posted by the District, subject to the Board's established rules.

U.S. Const. Am. I

B. Public Interaction.

The Board approves the following rules for public interaction with District-owned social media accounts that are designated public forums and directs staff to post this information on the District website and all such social media accounts:

The District encourages community members to respond to posts and share comments that are constructive and courteous toward the school community. Statements and opinions expressed by visitors to the account do not reflect the opinions of the District. Questions regarding information should be directed to the building principal or to the Superintendent's office for district-wide information. The District shall review comments and may remove comments which:

1. Are profane, vulgar, harmful to minors or obscene, in accordance with Board policy.
2. Contain threats or contain personal attacks on individuals in the school community.
3. Promote, suggest or encourage illegal activity or incite violence.
4. Promote or endorse commercial products, services or businesses.
5. Contain confidential information.
6. Contain false or libelous statements.
7. Contain language that causes a disruption to the school environment or operations.
8. Contain hate speech directed at a protected class of individuals, in accordance with Board policy on discrimination and harassment.
9. Are discriminatory or harassing or contain comments or imagery that attack or mock an individual due to his/her real or perceived race, color, national origin/ethnicity, age, creed, disability/handicap, sex (including discrimination on the basis of sex stereotypes, sex characteristics, pregnancy or related conditions, sexual orientation, and gender identity), marital status, family status, religion, genetic information, or any other legally protected classification.
10. Are spamming in nature (*i.e.,* same comment posted repeatedly).
11. Contain links to external websites.

C. Training.

All District staff assigned to monitor and maintain District-owned social media accounts shall receive training on:

1. Regularly reviewing District-owned social media accounts, in coordination with the District's chief communications representative, to update, remove and/or correct information.

20 U.S.C. § 1232g; 34 C.F.R. Part 99

2. Complying with confidentiality provisions of student and staff information, in accordance with applicable law, regulations and Board policy and administrative regulations.

3. Monitoring content for confidentiality and intellectual property violations, documenting potential violations, and notifying appropriate District staff to consider further action.

4. Monitoring content for web accessibility standards and responding to public requests for accommodations.

5. Monitoring public comments and responding, where appropriate, with clarification or redirection to additional information.

6. Monitoring public comments according to the Board's established rules, documenting potential violations, and notifying appropriate District staff to consider further action. Staff shall be provided training to assess comments in a viewpoint neutral manner, based on the Board's approved rules, regard-ess of the specific subject matter of comments.

D. Removal of Posts.

The Board authorizes designated District staff maintaining District-owned social media accounts to remove individual posts or comments by public users that violate the established social media rules of this policy. The Board directs that review and consideration of posts or comments shall not discriminate on the basis of content or viewpoint, and staff must always be able to articulate the reason for removing a specific post, in accordance with Board policy. Staff may consult with the Superintendent or designee and the school solicitor in determining appropriate actions. Posts and comments may not be removed solely because they are critical of the District or District leadership, because they promote an unpopular opinion, or because of their viewpoint if the post or comment otherwise complies with the established social media rules.

Designated District staff may not block users from accessing or commenting on District-owned social media accounts unless the outside account is identified as a security or system threat or spam account. Staff may consult with the Superintendent or designee and the school solicitor in determining appropriate actions for people who violate the rules for public interaction with District social media accounts for further investigation and potential legal remedies.

The School District may delete certain of its social media posts, in their entirety and including all comments, at the discretion of the District's administration. The District has no obligation to maintain its social media posts in perpetuity and their temporary presence on the internet is not a warranty of their future presence.

District social media accounts must remain professional, and consistent with the educational mission of the School District at all times. The operators of the District social media accounts are responsible for the content on the social media accounts that they manage.

E. Personally Identifiable Information.

The Board authorizes posting of student images in photos or videos depicting the educational process or school-related events on District-owned social media accounts for publicity purposes, unless the students' parents/guardians have opted out of sharing directory information under the Family Educational Rights and Privacy Act and Board policy, or have opted out of the District's Photography Release Form.

The Board prohibits posting of other personally identifiable information of students on District-owned social media accounts without the consent of the parent/guardian, in accordance with applicable law, regulations and Board policy.

The Board prohibits posting of staff images in photos or videos when a staff member has submitted a request to the Superintendent or designee that their image not be posted.

28 C.F.R. § 35.160

F. Accessibility.

The Board directs District staff who maintain District-owned social media accounts to post content that is accessible to individuals with disabilities, to the greatest extent possible based on the limitations of the platform. This shall include, but is not limited to:

1. Including alternate text descriptions or captions for images.

2. Including captions for video content.

3. Avoiding text that is posted as an image.

4. Creating links and attachments in formats that are accessible to screen readers and other assistive technology.

5. Formatting text so that it is accessible to screen readers and other assistive technology.

All District-owned social media accounts shall contain clear contact information that may be used by members of the public to request accommodations or assistance.

G. Intellectual Property Rights.

The illegal use of copyrighted, branded or trademarked materials or trade secrets is prohibited on District-owned social media accounts. All content shall be subject to copyright fair use guidelines and applicable laws, regulations and Board policy.

6. Other Social Media Accounts

A. Connecting District Accounts to Other Accounts.

Content or information posted to District-owned social media accounts shall not be connected to other social media accounts through linking or tagging if the outside account is for a commercial application, product or service and the District or its employees would receive financial or other compensation as a result of the connection.

District-owned social media accounts may be connected through linking or tagging to social media accounts of parent-teacher organizations, District-related booster organizations or similar school-related groups when the content or information has been reviewed and approved by the Principal/ Superintendent.

B. Personal Social Media Accounts.

The District shall not authorize, endorse or participate in posting on private social media accounts of individual school directors or school employees.

School directors and employees are strongly encouraged to use privacy settings on social media accounts and to clearly identify that it is their personal social media account and that it does not officially represent the Board or District.

School employees should only communicate with students through District-provided communication devices or platforms. School District employees are urged to exercise extreme caution before communicating with students via social media. Such electronic communication may cross professional boundaries in violation of the Pennsylvania Code of Professional Practice and Con-

22 Pa Code ch. 235; School Code § 2070.1 *et seq.*

duct for Educators, and the Educator Discipline Act. School District employees are urged to maintain strict professional boundaries on social media, and to protect against even the appearance of impropriety.

Pickering v. Board of Education, 391 U.S. 563 (1968)

The District respects employees' freedom of expression. The District does not actively monitor personal social media accounts of current school employees; however, the District reserves the right to address employees' job-related speech or employee speech posted on social media that has the potential to affect the District's operations. Speech that takes place off-site and on an employee's own time, including posting on personal social media accounts, may be addressed if the District establishes that the employee's expression infringed on the interests of the District in promoting the efficient and effective functioning and educational purpose of the District. If employee speech or expression would violate law or Board policy in a traditional forum, it is also prohibited in an online forum. When an employee speaks as a citizen on a matter of public concern, the District shall consult with the school solicitor in determining the appropriate course of action, in accordance with applicable law, regulations and Board policy.

Student use of personal social media accounts shall be addressed in accordance with applicable Board policies related to student conduct, expression and students' individual rights and responsibilities. In accordance with Board policy, the District shall provide education on network etiquette and appropriate online behavior for students, including interaction with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

7. Use of Artificial Intelligence

Artificial Intelligence ("AI") in education is the use of AI technologies within the classroom and offices to enhance teaching and learning and improve productivity, More specifically, generative AI tools offer significant educational benefits but also pose risks that must be managed. Generative AI refers to systems that create new content based on learned patterns. This Policy applies to all AI used in education, administration, and operations. Users must also comply with all other District policies on technology use, data protection, or academic integrity.

Key principles include using AI to enhance educational goals, ensuring equitable access, promoting AI literacy, addressing risks such as misinformation and bias, maintaining academic integrity, and conducting regular audits. Responsible AI use varies by context, and teachers will clarify when and how AI tools are used. Prohibited uses include AI for bullying, plagiarism, and privacy violations. The District recognizes the importance of human oversight and accountability in AI applications and implements security measures to protect data and privacy.

8. Prohibitions

The use of the District Network, Internet, or any school or school-provided computers, smartphones, tablets, or other devices, applications, or systems 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.

Prohibited actions include:

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

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

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

D. 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.

E. 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.

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

G. 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.

H. 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.

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

J. Destruction, modification, abuse, or unauthorized access to district computer hardware, software, or files, including, but not limited to, loading, downloading, or use of unauthorized games, programs, files, or other electronic media.

K. Destruction of district computer hardware or software.

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

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

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

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

P. 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.

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

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

S. Use of equipment in any manner that would disrupt network use by others, including but not limited to the propagation of computer "viruses", "worms", "Trojan horses", and trapdoor program codes.

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

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

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

W. 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.

X. Use of a computer that has been logged in under another user's name or account, 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.

Y. Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate.

Z. Use that conceals or attempts to conceal a user's identity, including use of anonymizers, or the impersonation of another user.

AA. Using technology resources to send any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business or educational interests.

BB. Use of District technology resources to tether or otherwise connect to a non-District owned device to access an unfiltered and/or unmonitored internet connection.

CC. Use of technology resources for political lobbying or campaigning, not including student elections (*e.g.*, student government, club officers, home-coming king/queen, etc.).

DD. The use of proxies or other means to bypass internet content filters and monitoring.

EE. The use of technology resources to gamble.

FF. The use of encryption software that has n ot been previously approved by the District.

GG. Use of technology resources to violate the law, facilitate illegal activity, or encourage others to do so, or violate any District policy.

HH. Use of technology resources to engage in any intentional act which might harm or threaten to harm the health, safety, or welfare of any person(s).

9. Consequences of Abuse of Responsibilities and Privileges	Any user of district technology resources who violates this policy, including, but not limited to, the prohibitions listed in Part 8 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, may have his or her user privileges temporarily or permanently 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 may be reported to the appropriate legal authorities for prosecution.
10. Limitation of Liability	The Catasauqua Area School District makes no warranties of any kind, either express or implied, for the service it is providing through its various technology resources. The District is not responsible, and will not be responsible, for any damages, including, 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, whether resulting from delays, non-deliveries, missed deliveries, service interruptions, or otherwise. Use of any information obtained via the District's technology resources is at the user's own risk.