

CLARENCE CENTRAL SCHOOL DISTRICT



District Technology Plan

July 2026 – June 2027

9625 Main Street

Clarence, NY 14031

Phone: 716-407-9100

Board of Education Approval: TBA

Contact:

Robert Raineri

Director of Technology

rraineri@clarenceschools.org

Phone: 716-407-9144

Fax: 716-407-9145

Plan URL: <https://www.clarenceschools.org/departments/information-technology/technology-plan>

Clarence Central School District Comprehensive Technology Plan

I. District Information

- The Clarence School District is located in the Town of Clarence in northeastern Erie County. Our offices are located in the High School at the intersection of Main Street and Gunnville Road.
- The district has four elementary schools, a middle school, and a high school. More than 380 teachers provide instruction to approximately 4,500 students across the District. Approximately 5% of the student population receives a free or reduced lunch.

II. Strategic Technology Planning & Committee

A. District Mission

The mission of the Clarence Central School District is *"to produce independent, lifelong learners who are responsible, contributing members of a diverse society."*

B. Technology Philosophy & Vision Statement

The Clarence Central School District believes that technology is integrated across the curriculum to motivate students and enhance learning. Information literacy and information technology are basic skills all Clarence students must possess by graduation to navigate a digital world and succeed in an information-based workplace.

The district is committed to providing state-of-the-art hardware and an effective support system to prepare lifelong learners who are ethical and responsible digital citizens. To transform this vision into reality, the following baseline conditions are necessary:

- **A Learning Environment providing:**
 - Convenient, easy-to-use access to global communications and technological resources.
 - Tools to demonstrate and enhance learning across all academic disciplines.
 - Opportunities to improve themselves and the world around them through technology.
 - Structural challenges to expand critical and creative thinking to the fullest potential.
 - Spaces for the active construction of meaning, reflection, and deep levels of understanding.
- **Students who will:**
 - Collaborate with others to process information and ideas to solve problems.
 - Access, manage, analyze, and communicate information through a wide variety of sources.
 - Apply technology to increase personal productivity and creativity.
 - Make morally and ethically sound choices regarding the uses of technology.
 - Remain self-directed and motivated to utilize technology as a lifelong tool for growth.
 - Strategize to isolate required data and solve unexpected logistical problems.
- **Staff Members who will:**
 - Achieve proficiency via ongoing professional development to manage information, integrate curriculum, and collaborate inside a professional learning community.
 - Maintain self-direction and utilize technology as a primary tool for personal professional development.
 - Develop targeted lesson activities and assessments incorporating student technology use to meet learning standards.

- Secure seamless access to necessary infrastructure and hardware resources.
- **Community Members who will:**
 - Access communications linking the school, home, and community.
 - Leverage educational opportunities to expand lifelong learning using school technology resources.
 - Benefit from graduating classes prepared as self-directed, technologically competent workers.

C. Mobile Device Provision

Dedicated Student Mobile Devices: Yes. At the start of the school year, the district provides a dedicated mobile device for every student across all grade levels.

D. District Technology Committee

- **Chairperson:** Superintendent of Schools
- **Committee Roster:**
 - District Staff:
 - Matt Frahm (*Superintendent*)
 - Kristin Overholt (*Assistant Superintendent*)
 - Patricia Grupka (*Assistant Superintendent*)
 - Robert Raineri (*Director of Technology*)
 - Benjamin Lathan, Michael Jacobson (*Microcomputer Specialists*)
 - Dawn Snyder, Tricia Andrews (*Board of Education Members*)
 - Elizabeth Chelus (*Assistant Principal, CMS*)
 - Kenneth Smith (*Principal, CHS*)
 - Kate Celej (*TOSA*)
 - Kathryn Green (*Director of Curriculum*)
 - **Community Members:**
 - Jon Brennan
 - Steven Duquette
 - Elizabeth Dunne (*CTA Union Leader*)
 - **Instructional Staff:**
 - Amy Ratajczak, Brian Schmidt, Deborah Wehrin, Heather Hartmann, Jason Urbanek, Katherine Lucia, Kathryn Wright, Kelly Barone, Matthew Andrews, Paul Cary, Ronald Kotlik, Rosalyn Vasi, Scott Gretch, Thomas Maroney, Andrew Johnston, Jessica Bork, Mari-Jo Gregor

III. Goal Attainment

The district evaluates its historical progress against the Statewide Learning Technology Plan vision across five diagnostic categories:

1. **Digital Content:** The District uses standards-based, accessible digital content supporting all curricula for all learners.
2. **Digital Use:** Learners, teachers, and administrators are proficient in using technology for educational achievement.
3. **Digital Capacity and Access:** The District's technology infrastructure completely supports learning and teaching across all educational environments.
4. **Leadership:** The District Instructional Technology Plan aligns fully with the Statewide Learning Technology Plan vision.
5. **Accountability:** District-level information is posted on the public website, remaining transparent, accessible, and easily understood by the community.

IV. Action Plan

Goal 1: Alignment & Impact

- **Goal Statement:** Ensure technology adoption aligns with instructional priorities, simplifies classroom practice, and is regularly reviewed for effectiveness.
- **Topic Alignment:** Classroom Technology (e.g., interactive boards, 3D printers, robotics, etc.)
- **Target Student Population:** All students
- **Additional Target Populations:** Teachers/Teacher Aides, Administrators, Parents/Guardians/Families/School Community, Technology Integration Specialists

Goal 2: Training & Support

- **Goal Statement:** Provide ongoing, differentiated professional learning on digital tools, AI, and instructional technology that balances innovation with teacher readiness.
- **Topic Alignment:** Professional Development
- **Target Student Population:** All students
- **Additional Target Populations:** Teachers/Teacher Aides, Administrators, Parents/Guardians/Families/School Community, Technology Integration Specialists

Goal 3: Wellness & Responsibility

- **Goal Statement:** Embed digital wellness and responsible use practices for staff and students through curriculum, counseling partnerships, and proactive supports.
- **Topic Alignment:** Other (Wellness & Responsibility)
- **Target Student Population:** All students
- **Additional Target Populations:** Teachers/Teacher Aides, Administrators, Parents/Guardians/Families/School Community, Technology Integration Specialists

Goal 4: District Expectations & Guidelines

- **Goal Statement:** Establish consistent districtwide guidelines for AI, Chromebook use, and classroom practices.
- **Topic Alignment:** Other (District Expectations & Guidelines)
- **Target Student Population:** All students
- **Additional Target Populations:** Teachers/Teacher Aides, Administrators, Parents/Guardians/Families/School Community, Technology Integration Specialists

V. Core Technical & PD Infrastructure Components

The district partitions its baseline management systems into three distinct institutional operational pillars:

1. **Teaching and Learning Infrastructure:** Focuses on integrating technology ethically to back mastery of learning standards. This includes standardized lesson planning, curriculum design, data analysis tools, hands-on tasks, and hardware/software verification protocols. Central office pre-vetting is strictly required for all purchases to ensure technical compatibility and alignment with broader district goals.
2. **Professional Development Plan:** Leverages internal mechanisms to build staff proficiency. Standard options include *My Learning Plan Courses*, *Technology Trainings by IT Staff*, *Timeout for Technology Sessions*, and active *Coaching and Mentoring* handled by the specialized Curriculum Team. The Curriculum Team consists of the Assistant Superintendent of Curriculum and Instruction, Director of Curriculum, and 6 Teachers on Special Assignment (TOSAs),

- supported by an expanded group of 47 elementary and secondary Department Chairpersons.
3. **Technical Infrastructure:** Encompasses the physical and digital core required to maintain operational stability. This includes the wide-area electronic backbone, switches, routers, connectivity protocols, firewalls, backup environments, security systems, server software, and dual broadband connections to the internet.

VI. NYSED Initiatives & Strategic Alignment

A. Comprehensive Student Performance Support

Clarence CSD leverages instructional technology to drive student performance, enforce academic standards, and ensure equitable access "everywhere, all the time". Guided by the local *Progress with Purpose* framework within the District's Strategic Plan, technology is intentionally integrated to enhance curriculum delivery, facilitate formative assessments, and supply data-informed instruction. Students leverage adaptive tools, assistive tech, and flexible learning environments to collaborate, create, and think critically. Short- and long-term funding streams protect device and internet equity while embedding responsible use expectations.

VII. Technology Integrated Curriculum

- **Prior to Completion of Grade 2:** Students will operate baseline computing infrastructure and tablets; use the digital library catalog to locate reading materials; securely log into networks with unique personal IDs; maintain password confidentiality; and demonstrate initial writing publication through media-rich digital resources under safe internet conditions.
- **Prior to Completion of Grade 5:** Students will practice responsible software use; research, collect data, and assemble targeted multimedia projects; conceptualize and manage group projects via digital planning tools with teacher guidance; apply calculators, data collection probes, and educational media for collaborative learning; and evaluate electronic sources for accuracy, bias, and relevance.
- **Prior to Completion of Grade 8:** Students will utilize productivity software and specialized peripherals; design, publish, and present custom digital media outputs (e.g., web pages, videos) to internal and external audiences; select correct technology resources to resolve real-world problems collaboratively; and practice exemplary digital citizenship across all research initiatives.
- **Prior to Completion of Grade 12:** Students will make informed choices among competing technical systems and cloud services to execute research, publication, and data analysis; collaborate with global peers or experts to construct content-specific knowledge repositories; advocate for legal and ethical behaviors (such as proper citation and copyright adherence) among peers and family; navigate complex human, cultural, and societal impacts of tech; justify tool selection based on efficiency; run curriculum-specific simulations; and author media-rich instructional presentations for younger students on digital ethics.

VIII. Administrative & Staffing Management Plan

A. District Personnel Allocation (Full-Time Equivalent Count)

Primary Staff Responsibility	District Employed Staff (FTE)	Staff Contracted Through Vendor/BOCES (FTE)	Total Combined FTE
District Technology Leadership	1.00	0.00	1.00
Instructional Support	1.60	0.00	1.60
Technical Support	4.00	0.80	4.80
TOTALS	6.40	0.80	7.40

B. Supplemental Administrative Requirements

- **Nonpublic School Computer Hardware Loans:** Yes. The district complies with Education Law Section 754 by actively facilitating the loan of instructional computer hardware to students legally attending nonpublic schools within district boundaries.

IX. Established Educational Technology Programs

The district documents multi-year innovation tracks across several specific fields. Implemented programs active for at least two consecutive years at the building or district level include:

- Advanced Computer Science or Technology Courses
- Instruction with Technology

X. Technology Access & Assistive Services

Clarence CSD maintains clear structural cooperation between the Special Education Department and the Technology Department to ensure individual accommodations are met following a student's Individualized Education Program (IEP) guidelines.

- **Available Assistive Hardware and Software Modifications:** Specially configured operating systems, document scanning, adaptive input/output switches, specialized laptop-based applications, wheelchairs, scooters, walkers, talking book readers, voice recognition software, screen readers, enlargement programs, automatic page turners, and adapted writing devices.
- **Scope of Assistive Services Provided:** Multi-disciplinary assistive technology evaluations; custom equipment leasing and configuration; continuous physical adjustments and equipment maintenance; specialized training programs for disabled individuals and their immediate families; and external technical training for professionals or employers involved in major life functions.

XI. Accountability & Evaluation

Governance of this plan is maintained through an annual review conducted by the district technology committee.

Appendix A: Technology Purchase Form Guide

Hardware/Software Request Form

This form is a digital request for hardware or software. Please be sure to have your funding source allocated already to expedite the process.

*** Quote Required for processing ***

Hi, Robert. When you submit this form, the owner will see your name and email address.

* Required

1. Who is funding the purchase? * 

☐ Building/Department

☐ PTO

☐ District Office

☐ Grant

☐ Other

2. Department Name 

3. Your Building? * 

☐ CHS

☐ CMS

☐ SH

☐ HH

☐ CC

☐ LV

☐ Special Education

☐ District Office

4. Who is the primary user? * 

☐ Faculty

☐ Staff

☐ Student

☐ Other

5. Name of Product * 

6. Type of Request * 

☐ New

☐ Upgrade

☐ Renewal

☐ Other

Appendix B: Procurement Workflows

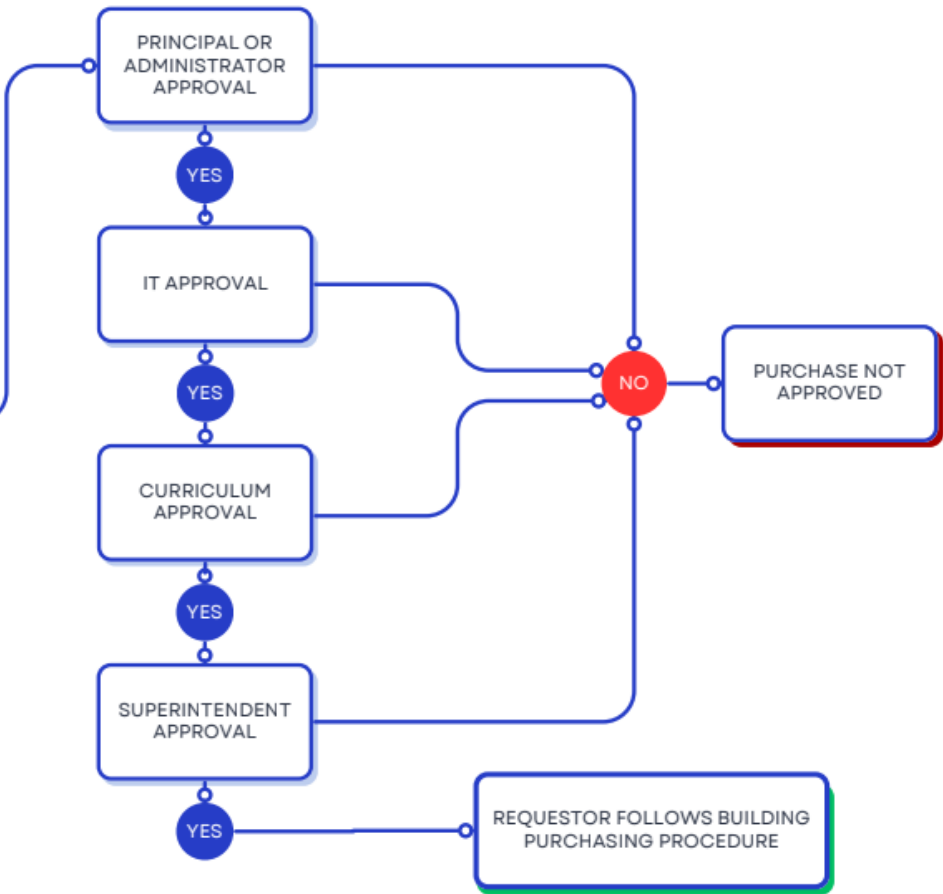
Technology
Purchase
Request and
Approval
Process

FACULTY/STAFF FILL
OUT DIGITAL
TECHNOLOGY
REQUEST FORM

QUOTE REQUIRED



[LINK TO
TECHNOLOGY
REQUEST FORM](#)



Appendix C: Acceptable Use Policy (AUP)

2026

7315
1 of 4

SUBJECT: ACCEPTABLE USE POLICY (STUDENT)

The District provides access to digital information systems through the District's computer network. This policy establishes acceptable use expectations, safeguards district information resources, and assists in compliance with applicable laws, regulations, and district procedures.

Definitions

For the purposes of this policy, the following definitions apply:

- a) "Digital information systems" means:
 - 1. All computer hardware, devices, and systems owned or leased by the District, including but not limited to:
 - (a) Computers of any size and form factor, including smartphones, tablets, and interactive whiteboards;
 - (b) Networks;
 - (c) Internet access;
 - (d) Network servers;
 - (e) Routers, cables, and switches;
 - (f) Video conferencing equipment; and
 - (g) Internet of things devices (devices that collect and share data, such as security systems or wearable devices); and
 - 2. Software that is owned, leased, or licensed by the District, or that the District has the use of through a cooperative services agreement (CoSer), and that is used to create, modify, store, or transmit information in a digitized form.

Overview

Prior to accessing district digital information systems all students must read, sign, and return the applicable acceptable use form(s). The District will provide reasonable oversight for their digital information systems, however, responsibility for their use ultimately lies with the individual user.

Students are provided with access to the District's digital information systems for the purpose of completing instructional assignments under the guidance of a teacher. Student use of the systems must comply with the standards in district policy, the District Code of Conduct, and/or other similar documents. Failure to comply may result in disciplinary action.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (STUDENT) (Cont'd.)

Except for any privilege or confidentiality recognized by law, students have no legitimate expectation of privacy during any use of the District's digital information systems or in any data on those systems. Any use may be monitored, recorded, or accessed in any manner by authorized personnel without additional prior notice to students. Periodic monitoring may be conducted of digital information systems used, including but not limited to, all computer files and all forms of electronic communication.

The District reserves the right to impose restrictions on the use of digital resources. For example, the District may block access to websites, services, or applications not serving legitimate business or educational purposes or may restrict users' ability to attach personal devices to the District's digital information systems or devices.

Acceptable Use

All student use of district digital information systems must comply with district policies, standards, procedures, and regulations, as well as any applicable federal and state laws and regulations, including, but not limited to, copyright laws and licensing agreements.

Acceptable student uses of the District's digital information systems include, but are not limited to:

- a) Protecting confidential information and student data, from unauthorized use or disclosure;
- b) Using digital information systems to support learning;
- c) Maintaining respectful conduct in their online communications and behavior;
- d) Reporting suspected cybersecurity incidents to appropriate district information technology personnel immediately; and
- e) Observing authorized levels of access and utilizing only approved digital information system devices and services.

In addition, students will ensure that their usage of the district digital information systems is aligned with the competencies of good digital citizenship. Students should be:

- a) Informed: evaluate the accuracy, perspective, and validity of digital media;
- b) Inclusive: open to hearing and recognizing multiple viewpoints and engaging others online with respect and empathy;
- c) Balanced: participate in a healthy variety of online activities and prioritize their time between virtual and physical activities;

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (STUDENT) (Cont'd.)

- d) Engaged: use technology and digital channels to solve problems and be a force for good in their community; and
- e) Alert: aware of their digital actions and know how to be safe online.

Unacceptable Use

The following list is not intended to be exhaustive but provides a framework for determining activities that constitute unacceptable use of district digital information systems.

Unacceptable student uses of the district digital information systems include, but are not limited to:

- a) Distributing, transmitting, posting, or storing any electronic communications, materials, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- b) Engaging in unauthorized use or disclosure of personal, private, sensitive, and/or confidential information, including entering this information into generative artificial intelligence (AI) or other AI systems;
- c) Connecting unapproved devices to the district digital information systems;
- d) Installing, downloading, or running software that has not been approved in accordance with district policies;
- e) Using district digital information systems for commercial or personal purposes, including solicitation or advertisement, in support of religious, political, not-for-profit organizations, or for-profit business activities;
- f) Providing unauthorized third parties access to the district digital information systems;
- g) Tampering with, disengaging, or otherwise circumventing district-implemented IT security;
- h) Plagiarizing or engaging in copyright infringement; and
- i) Using district digital information systems to access personal social media platforms, email, or other personal account-based platforms.
- j.) Engaging in any personal use of the district digital information systems.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (STUDENT) (Cont'd.)

Individual Accountability

Individual accountability is required when accessing all district digital information systems. Student users must comply with district procedures and any other applicable district documents for data networks and security access which may include password protocols, use of multi-factor authentication, and other security measures as defined by the District. All student users must treat their credentials as confidential information which must not be disclosed or shared. All student users are responsible for protecting against unauthorized activities performed under their user ID, devices, or any other district system.

Compliance

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The District will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

NOTE: Refer also to Policies #7316 -- Use of Internet-Enabled Devices During the School Day
#8271 -- Internet Safety/Internet Content Filtering
District Code of Conduct

Adoption Date

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL)

The District provides access to digital information systems through the District's computer network. This policy establishes acceptable use expectations, safeguards district information resources, and assists in compliance with applicable laws, regulations, and district procedures.

Definitions

For the purposes of this policy, the following definitions apply:

- a) "Digital information systems" means:
 - 1. All computer hardware, devices, and systems owned or leased by the District, including but not limited to:
 - (a) Computers of any size and form factor, including smartphones, tablets, and interactive whiteboards;
 - (b) Networks;
 - (c) Internet access;
 - (d) Network servers;
 - (e) Routers, cables, and switches;
 - (f) Video conferencing equipment; and
 - (g) Internet of things devices (devices that collect and share data, such as security systems or wearable devices); and
 - 2. Software that is owned, leased, or licensed by the District, or that the District has the use of through a cooperative services agreement (CoSer), and that is used to create, modify, store, or transmit information in a digitized form.
- b) "Personnel" means all district employees, substitutes, contractors, consultants, student teachers, volunteers, and any other individuals granted access to district digital information systems.

Overview

Prior to accessing these digital information systems, all personnel must read, and/or acknowledge the applicable acceptable use form(s). The District will provide reasonable oversight for their digital information systems, however, responsibility for their use ultimately lies with the individual user.

(Continued)

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)

Except for any privilege or confidentiality recognized by law, district personnel have no legitimate expectation of privacy during any use of the District's digital information systems or in any data on those systems. Any use may be monitored, recorded, or accessed in any manner by authorized personnel without additional prior notice to personnel. Periodic monitoring may be conducted of digital information systems used, including, but not limited to, all computer files and all forms of electronic communication.

The District reserves the right to impose restrictions on the use of particular digital resources. For example, the District may block access to websites, services, or applications not serving legitimate business or educational purposes or may restrict users' ability to attach personal devices to the District's digital information systems or devices.

Acceptable Use

All uses of district digital information systems by district personnel must comply with district policies, standards, procedures, and regulations, as well as any applicable federal and state laws and regulations, including but not limited to copyright laws and licensing agreements.

Acceptable uses of the district digital information systems include, but are not limited to, the following:

- a) Protecting confidential information and student data from unauthorized use or disclosure;
- b) Using digital information systems to support student learning and district business operations;
- c) Maintaining professional conduct in online communications and behavior as in all other aspects of work;
- d) Reporting suspected cybersecurity incidents to appropriate district information technology personnel immediately; and
- e) Observing authorized levels of access and utilizing only approved digital information system devices and services.

Unacceptable Use

The following list is not intended to be exhaustive, but provides a framework for determining activities that constitute unacceptable use of district digital information systems.

(Continued)

Personnel

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)

Unacceptable uses of the district digital information systems include, but are not limited to, the following:

- a) Distributing, transmitting, posting, or storing any electronic communications, materials, or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate;
- b) Engaging in unauthorized use or disclosure of personal, private, sensitive, and/or confidential information, including entering this information into generative artificial intelligence (AI) or other AI systems;
- c) Connecting unapproved devices to the district digital information systems;
- d) Installing, downloading, or running software that has not been approved in accordance with district policies;
- e) Using district digital information systems for commercial or personal purposes, including solicitation or advertisement, in support of religious, political, not-for-profit organizations, for-profit business activities, or in support of other outside employment or business activity;
- f) Providing unauthorized third parties access to the district digital information systems;
- g) Tampering with, disengaging, or otherwise circumventing district-implemented IT security;
- h) Plagiarizing or engaging in copyright infringement; and
- i) Using district digital information systems to access personal social media platforms, email, or other personal account-based platforms.

Occasional and Incidental Personal Use

The District permits occasional and incidental personal use of its digital information systems, provided the use is consistent with this policy, is limited in amount and duration, does not conflict with the user's ability to perform their duties, and does not impede the ability of other users to utilize the system for legitimate work purposes, including but not limited to, extensive bandwidth, resource, or storage utilization. The District may revoke or limit this permission at any time.

(Continued)

Personnel

SUBJECT: ACCEPTABLE USE POLICY (PERSONNEL) (Cont'd.)**Individual Accountability**

Individual accountability is required when accessing all district digital information systems. Users must comply with district procedures and any other applicable district documents for data networks and security access which may include password protocols, use of multi-factor authentication, and other security measures as defined by the District. All users must treat their credentials as confidential information which must not be disclosed or shared. All users are responsible for protecting against unauthorized activities performed under their user ID, devices, or any other district system.

Compliance

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The District will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#5676 -- Privacy and Security for Student Data and Teacher and Principal Data
#5850 -- Data Networks and Security Access
#5851 -- Cybersecurity Incident Response
#6411 -- Use of Email in the District
#6412 -- Social Media Use
#8271 -- Internet Safety/Internet Content Filtering

Adoption Date

Appendix D: Internet Safety / Content Filtering Policy

In compliance with the Children's Internet Protection Act (CIPA) and Regulations of the Federal Communication Commission (FCC), the District will ensure the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. These technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. The District will provide for the education of students regarding appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response. Further, appropriate monitoring of online activities of minors, as determined by the building or program supervisor, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the Board's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate instructional materials and activities to enhance the school's programs; and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minor to inappropriate matter on the Internet may include, but will not be limited to, the following guidelines:

- a) Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail, chat rooms, as well as social networking websites, may be blocked as deemed necessary to ensure the safety of students;
- b) Monitoring logs of access in order to keep track of the websites visited by students as a measure to restrict access to materials harmful to minors;
- c) In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and
- d) Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal identification information regarding such students.

(Continued)

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING (Cont'd)

The determination of what is “inappropriate” for minors will be determined by the District and/or designated school official(s). It is acknowledged that the determination of “inappropriate” material may vary depending upon the circumstances of the situation and the age of the students involved in online research.

The terms “minor,” “child pornography,” “harmful to minors,” “obscene,” “technology protection measure,” “sexual act,” and “sexual contact” will be as defined in accordance with CIPA and other applicable laws or regulations as may be appropriate.

Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the District.

The District will provide certification, pursuant to the requirements of CIPA, to document the District’s adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking or filtering of access to certain material on the Internet) for all District computers with Internet access.

Internet Safety Instruction

In accordance with New York State Education Law, the District may provide, to students in grades K through 12, instruction designed to promote the proper and safe use of the Internet. The Commissioner will provide technical assistance in the development of curricula for this course of study which will be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.

Under the Protecting Children in the 21st Century Act, students will also be educated on appropriate interactions with other individuals on social networking websites and in chat rooms, as well as cyberbullying awareness and response.

Access to Inappropriate Content/Material and Use of Personal Technology of Electronic Devices

Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students.

Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student’s own personal technology or electronic device on school grounds or at school events.

(Continued)

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING (Cont'd)

The District is not responsible for inappropriate content or material accessed via a student's own personal technology or electronic device or via an unfiltered Internet connection received through a student's own personal technology or electronic device.

Notification/Authorization

The District's Acceptable Use Policy will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet.

The District has provided reasonable public notice and has held at least one (1) public hearing or meeting to address the proposed Internet Safety/Internet Content Filtering Policy prior to Board adoption. Additional public notice and a hearing or meeting is not necessary when amendments are made to the Internet Safety Policy in the future.

The District's Internet Safety/Internet Content Filtering Policy must be made available to the FCC upon request. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of this policy as well as any other District policies relating to the use of technology.

The Internet Safety/Internet Content Filtering Policy is required to be retained by the school for at least five (5) years after the funding year in which the policy was relied upon to obtain E-rate funding.

47 USC §§ 254(h) and 254(1)
47 CFR Part 54
Education Law § 814

NOTE: Refer also to Policy #7315 – Student Acceptable Use Policy
#7316 – Student Use of Personal Technology
District Code of Conduct

Appendix E: Current Hardware Inventory Statistics

Count	Model Type
547	Access Point
46	Cart
6598	Chromebook
52	Chromebox
259	Desktop
4	Digital Camera
430	Display
5	Dock
231	Document Camera
2	DVD Player
11	DVD VHS Combo Player
228	EPSON Brightlink
1	External Hard Drive
2	IA Display
7	IAWB Physical Board
1	Label Maker
1490	Laptop
1	LaserDisc Player
45	Monitor
5	Network Extender
176	Peripheral
671	Phone
226	Printer
164	Projector
144	Scanner
60	Server
1	Service Cart
4	Short Throw Projector for IAWB
62	Sound Equipment
202	Switch/Router
483	Tablet
8	Temperature Scanner
352	Thin Client
75	UPS
4	VHS Player
12	Video Camera
20	Webcam
12629	Total

Appendix F: Student Device Replacement Cycle Chart

Student Chromebook Replacement Cycle

	3100		3110		3120	3100 EOL			3110 EOL
	21-22	22-23	23-24	24-25	25-26	26-27	27-28	28-29	29-30
K	2034	2035	2036	2037	2038	2039	2040	2041	2042
1	2033	2034	2035	2036	2037	2038	2039	2040	2041
2	2032	2033	2034	2035	2036	2037	2038	2039	2040
3	2031	2032	2033	2034	2035	2036	2037	2038	2039
4	2030	2031	2032	2033	2034	2035	2036	2037	2038
5	2029	2030	2031	2032	2033	2034	2035	2036	2037
6	2028	2029	2030	2031	2032	2033	2034	2035	2036
7	2027	2028	2029	2030	2031	2032	2033	2034	2035
8	2026	2027	2028	2029	2030	2031	2032	2033	2034
9	2025	2026	2027	2028	2029	2030	2031	2032	2033
10	2024	2025	2026	2027	2028	2029	2030	2031	2032
11	2023	2024	2025	2026	2027	2028	2029	2030	2031
12	2022	2023	2024	2025	2026	2027	2028	2029	2030