CLARENCE CENTRAL SCHOOL DISTRICT

District Technology Plan

July 2021 – June 2024

9625 Main Street

Clarence, NY 14031

Phone: 716-407-9100

Board of Education Approval: July 12, 2021

Contact:

Robert Raineri
Senior Microcomputer Technical Support Specialist
rraineri@clarenceschools.org
Phone: 716-407-9144
Fax: 716-407-9145
Plan URL: https://www.clarenceschools.org/Page/108

Table of Contents

INTRODUCTION

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 classroom instruction to 5,000 students across the District. Approximately 5% of the student population receives a free or reduced lunch.

The technology plan is in its sixth revision and conforms to the District's overall mission: "to produce independent, lifelong learners who are responsible, contributing members of a diverse society." The plan is available for viewing through the District website or upon request in our District Office.

The committee responsible for this revision of the plan is shown in the table below:

District Technology Committee	
Name	**Position**
Amy Ratajczak	Speech
Andrea Benkovich	Grade 4 — LV
Andrew Johnston	Librarian — CHS
Benjamin Lathan	Microcomputer Specialist
Brian Schmidt	Business — CHS
Charles Kohler	Tech Ed — MS
Christine Hanlon	Science — MS
Dawn Snyder	Board of Education Member
Deborah Wehrlin	Science — MS
Debra Crahen	Grade 2 — SH
Elizabeth Chelus	Assistant Principal — CMS
Elizabeth Dunne	CTA Union Leader
Finune Shaibi	CIO and Curriculum Coordinator
Geoffrey Hicks	Superintendent
George Gilham	Art — CHS
Heather Hartmann	Business — CHS
Jason Urbanek	Technology Education — CHS
Jessica Bork	Librarian — MS
Jon Brennan	Community/Business Rep
Kate Celej	TOSA
Katherine Lucia	LOTE — MS
Kathryn Wright	Science — MS

Kelly Barone	LOTE — MS
Kenneth Smith	Principal — CHS
Kimberly Zabel	Grade 5 — CC
Kristin Overholt	Assistant Superintendent
Margaret Aldrich	Elementary Principal
Mari-Jo Gregor	Librarian — LV
Mary Schnitter	Grade 5 — HH
Matt Stock	Parent — IT Specialist
Matthew Andrews	Social Studies—CHS
Michael Jacobson	Microcomputer Specialist
Michelle Layer	Grade 5 — CC
Paul Cary	Grade 6 — CMS
Robert Raineri	Sr Microcomputer Specialist
Ronald Kotlik	Social Studies — CHS
Rosalyn Vasi	Grade 2 — SH
Scott Gretch	Art — HH
Steven Duquette	Community Representative
Thomas Maroney	Technology Education — CHS
Tricia Andrews	Board of Education Member
Erin Tinklepaugh	Student Member (Senior 20-21)
Sarah Beckage	Student Member (Senior 20-21)
Grace Lipinski	Student Member (Senior 20-21)

TECHNOLOGY PHILOSOPHY

The Clarence Central School District believes that technology is integrated across the curriculum. We believe technology can motivate students and enhance learning. Technologically literate students will be able to navigate in a digital world.

Information literacy and information technology are basic skills all Clarence students need to have by the time they graduate. The ability to navigate information is of critical importance for students today who are living and learning in an information society and who, as citizens of tomorrow, will be earning a living in an information-based workplace.

TECHNOLOGY VISION STATEMENT

The CCSD is committed to accomplishing its mission to prepare lifelong learners who are ethical and responsible digital citizens.

CCSD members will be able to use technology to retrieve and manage information, communicate in a variety of modes, solve problems creatively, think critically, remain flexible and continue to learn. CCSD members will be self-directed citizens able to thrive in a rapidly changing world.

The CCSD is committed to providing state-of-the-art technology hardware and an effective support system to maintain equipment and respond to our users.

To transform the Clarence philosophy and vision into reality for students, the following conditions are necessary:

A **Learning Environment** in which all involved will have:

- access to convenient and easy to use global communications and technological resources,
- the technological tools to demonstrate and enhance learning across all disciplines,
- opportunities to improve themselves and the world around them through the use of technology,
- challenges to develop their critical and creative thinking to the fullest potential,
- opportunities 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,
- become lifelong learners who can access, manage, analyze and communicate information through a wide variety of sources,
- use technology to enhance creativity and productivity,
- make decisions concerning the uses of technology that are morally and ethically sound,
- be self-directed and motivated to learn, utilizing the technology as a “tool” for lifelong learning and personal development,
- strategize to get needed data and find answers using resources to solve problems that they encounter.

Staff members who will:

- become proficient through professional development opportunities in the use of technology to develop learning opportunities for students, manage information, integrate curriculum, and collaborate with colleagues in a learning community,
- be self-directed and motivated to learn, utilizing technology as a tool for lifelong learning and personal development,
- develop lesson activities and assessments that incorporate student use of technology in order to demonstrate learning standards,
- have access to the necessary resources for technology, which will include the implementation of technology.

Community members who will:

- have access to communications that will connect the school, home and community,
- have the educational opportunities to enhance lifelong learning through the use of technology in the schools,
- benefit from students prepared as self-directed citizens and technologically competent workers.

TECHNOLOGY PLAN: KEY COMPONENTS

The Technology Committee identified three key components of the revised technology plan. The key components are:

1) **Teaching and Learning Infrastructure:** refers to the use of technology to support students and their demonstration of the learning standard mastery:
   - curriculum and assessment design,
   - lesson planning,
   - best instructional models,
   - hands-on tasks,
   - products that demonstrate knowledge and skills,
   - technology for data management and analysis.

   The teaching and learning component is at the heart of the district's purpose and mission. This key component includes the knowledge and skill necessary to use technology ethically. This component would include the practice of ethical standards when using technology and respect for the principles of intellectual freedom and property rights.

   The component also includes professional development. It is imperative that teachers and staff members receive high quality, ongoing training in order to utilize technology in support of the teaching and learning process. The professional development component includes all the strategies necessary to train staff, as well as a description of the essential skills that must be acquired in order to be technologically literate.

   Also included are the hardware and software necessary to support teaching and learning in the school district. It considers the potential configurations of hardware at each level, whether it is a computer lab, clusters of computers or other devices in a classroom, wireless carts of laptops, tablet computers, or stand-alone machines. The component also recognizes the importance of the Internet as a means for delivering content to support the processes of teaching and learning.

2) **Professional Development Plan:** refers to the plan for educators and administrator's attainment of the instructional technology vision such as:
    - My Learning Plan Courses,
    - Technology Trainings by IT Staff,
    - Timeout for Technology Sessions,
    - Coaching and Mentoring by Curriculum Team

Through the purchases of mobile devices within the classroom, we provide another avenue for students to communicate and collaborate in the learning process. Access to information is vital to the success of students, teachers, administrators and parents. Web-based applications and online learning communities (i.e. Schoology) open a window for all stakeholders to enter the District's learning environment in a safe and secure manner. Administrators, teachers, parents and students are able to access this environment for multiple purposes including access to coursework, District and building information and to participate in a District-wide virtual learning community.

The District will focus professional development opportunities around technology integration in numerous ways, including K-12 District-wide staff development and embedded classroom learning experiences. The Curriculum team will act in a lead role in the development, planning and execution of these opportunities for faculty and staff based on the needs of our District stakeholders. The Curriculum team, consisting of Director of Curriculum and two Teachers on Special Assignment, will have a specific focus on providing a coaching and mentoring model to teachers and will be essential in assessing the needs, prioritizing those needs and creating innovative solutions to help better assist teachers in their professional growth within technology integration. The Curriculum Team will also provide facilitation to a now expanded District Department Chairpersons that will consist of 47 elementary and secondary teachers to provide guidance and further support in the implementation of these technology initiatives across the District.

3) **Technical Infrastructure**: is inclusive of everything that is needed to make the technology work, such as:
    - electronic backbone for the school district wide-area,
    - routers and switches that connect the network,
    - wireless, wiring and connectivity protocols,
    - servers and software,
    - security systems, backup systems and firewall
    - dual broadband connections to the internet through Erie 1 BOCES

Each key component of the technology plan delineates a series of goals and action steps that define activities to be accomplished, the time frame by which the activities will be accomplished, the budgeted funds for each activity, and how each goal will be evaluated. The technology plan contains six major goals, which are listed below along with the key component to which they relate:

DISTRICT GOALS, NYSSED GOALS, AND ACTION PLAN

Key Component: Teaching & Learning Infrastructure

Goal 1: Cultivate a technology-rich environment to support and enhance teaching and learning.

Goal 2: Students use technology regularly to demonstrate learning and communicate in a digital world.

Goal 3: All students and educators will have access to a robust and comprehensive infrastructure when and where they need it for learning.

Key Component: Technical Infrastructure

Goal 4: The learning and technical infrastructure is accessible and equitable throughout the district and addresses evolving needs of all stakeholders.

Key Component: Professional Development

Goal 5: An enhanced professional development system exists for all teachers to foster growth and continuous improvement of technology integration.

All technology related purchases must be approved at a central office level. Individual buildings and/or teachers cannot make purchases related to technology without properly vetting the purchase for compatibility with existing systems and adherence to the Technology Plan goals.

CCSD and NYSED Instructional Technology Goals Crosswalk

	CCSD Goal	NYSED Goal	Targeted Population	Action Plan
Goal 1	**Cultivate a technology-rich environment to support and enhance teaching and learning.**	Develop a strategic vision and goals to support student achievement and engagement through the seamless integration of technology into teaching and learning.	All Teachers, Staff, and Students	Utilize digital content management tools (e.g., Schoology) to support instructional, assessment, and curriculum design practices.
				Utilize digital tools to communicate, collaborate, design, plan and reflect on teaching and learning.
				The district uses instructional technology to strengthen relationships and connections with families to assist in building a culturally responsive learning environment to enhance student learning.
				Utilize digital tools to promote positive interactions and exchange ideas and strategies between teachers, students, and parents.
				Evaluate current technologies and district wide software system to coordinate budget planning process.
Goal 2	**Students use technology regularly to demonstrate**	Provide access to relevant and rigorous professional	All Students	Evaluate and collect exemplary models of innovative technology ideas/practice.
				Working towards common assessments in every course that

	learning and communicate in a digital world.	development to ensure educators and leaders are proficient in the integration of learning technologies.		include the integration of essential technology skills.
				Create learning tasks/activities that include the mandatory integration of essential technology skills in unit design.
				Utilize digital tools to communicate, collaborate, design, plan and reflect on teaching and learning.
Goal 3	**All students and educators will have access to robust and comprehensive digital resources when and where they need it for learning.**	Increase equitable access to high-quality digital resources and standards-based, technology-rich learning experiences.	All Teachers, Staff, and Students	Maintain different mobile platforms to provide flexibility for technology and usage.
				Ensure equitable distribution of technology resources across the six schools in the district.
				Support cloud-based and virtual systems that allow students and teachers to access and use digital resources remotely.
				Evaluate annually the effectiveness of student learning software and digital resources.
Goal 4	**The learning and technical infrastructure is accessible and equitable throughout the district and addresses evolving needs of all stakeholders.**	Design, implement, and sustain a robust, secure network to ensure sufficient, reliable high-speed connectivity for learners, educators, and leaders.	All Teachers, Staff, and Students	The infrastructure and installed base of equipment is regularly monitored, repaired, and replaced when necessary.
				A technology support system exists that addresses user needs and maintains the infrastructure.
				The technical infrastructure delivers reliable, fast, and secure access to applications, platforms, and the Internet.
				All grade levels and departments have access to mobile devices sufficient to meeting targeted learning goals.
Goal 5	**An enhanced professional development system exists for all teachers to foster growth and continuous improvement of technology integration.**	Provide access to relevant and rigorous professional development to ensure educators and leaders are proficient in the integration of learning technologies.	All Teachers, Staff, and Students	Include technology professional development opportunities that relate to data collection and analysis through the use of technology.
				Professional development consisting of virtual, blended, and face-to-face learning communities will be available.
				Educators will be supported by technology that connects them to people, data, content, resources, expertise, and learning experiences.
				The district uses instructional technology to assist in varying teaching approaches to accommodate diverse learning styles and language proficiencies.

SUGGESTED TECHNOLOGY INTEGRATED CURRICULUM

Prior to the Completion of Grade 2 students will:

- Use devices to successfully operate computers, tablets, and other technologies
- Use OPAC to locate a book for independent reading
- Demonstrate an ability to log into the network with a personal ID, run network software, and respect privacy of all other users by only using their personal ID
- Practice responsible use of appropriate technology and curriculum related software
- Understand and practice safe Internet usage
- Communicate technology ideas using developmentally appropriate and accurate terminology
- Publish different forms of writing using digital tools and media-rich resources

Prior to the completion of Grade 5 students will:

- Practice responsible use of appropriate technology and curriculum related software
- Research, collect data, and create a curriculum related multimedia project
- Conceptualize, guide, and manage individual or group learning projects using digital planning tools with teacher support
- Communicate about technology using developmentally appropriate and accurate terminology
- Use technologies (i.e. calculators, data collection probes, videos, educational software, Internet) for research, problem-solving, self-directed learning, and collaborative learning activities
- Evaluate the accuracy, relevance, appropriateness, comprehensiveness, and bias of electronic information sources

Prior to the completion of Grade 8 students will:

- Apply productivity/multimedia tools and peripherals to support personal productivity, group collaboration, and learning throughout the curriculum
- Design, develop, publish, and present products (e.g. web pages, videos, etc.) using technology resources that demonstrate and communicate curriculum concepts to audiences inside and outside the classroom
- Select and use appropriate tools and technology resources to collaboratively accomplish a variety of tasks and solve problems
- Research and evaluate the accuracy, relevance, appropriateness, comprehensiveness, and bias of electronic information sources while working on solutions to real world problems
- Practice and demonstrate exemplary digital citizenship principles as a part of all Internet research and technology-based classroom projects
- Use of technology as part of classroom instruction and Internet research to enhance learning

Prior to the completion of Grade 12 students will:

- Make informed choices among technology systems, resources, and services to meet the need for collaboration, research, publication, communication, and productivity
- Select and apply technology tools for research, information analysis, problem-solving, and decision-making in content learning

- Collaborate with peers, experts, and others to contribute to a content related knowledge base by using technology to compile, synthesize, produce, and disseminate information, models, and other creative works
- Demonstrate and advocate for legal and ethical behaviors among peers, family, and community regarding the use of technology and information when selecting, acquiring, and citing resources
- Demonstrate understanding of human, cultural, and societal issues related to technology
- Select digital tools and resources for use in real-world tasks and justify their selection based on their efficiency and effectiveness
- Employ curriculum specific simulations to practice critical-thinking processes
- Create media-rich presentations for other students on the appropriate and ethical use of digital tools and resources

TECHNOLOGY ACCESS FOR ALL STUDENTS AND TEACHERS

The district will continue to provide support for students with special needs and students requiring assistive technology as a part of their educational program. A continuing cooperative effort between the District Special Education Department and the District Technology Department will be maintained to ensure all students and teachers will have their technology needs met in the most effective way possible. An adaptive technology liaison from special education will work with an identified technology support person to develop solutions for students on an individual basis. The student's Individual Education Program will be used as a guideline. Services of this type include:

- Specially configured software
- Document Scanning
- Use of adaptive devices
- Special laptop-based applications

Student–based solutions continue to be reviewed on a regular basis. The adaptive technology liaison will attend monthly technology department meetings to discuss solutions being developed for specific students and special application areas.

The district will identify assistive technology devices and assistive technology services necessary to facilitate the success and independence of students with disabilities in academic, social, communication, occupational and recreational activities.

Use of assistive technology addresses students' barriers to learning and can reduce a student's reliance on parents, siblings, friends and teachers, helping them to transition into adulthood. Assistive technology for individuals with sensory, mobility, cognitive and learning disabilities should provide them with the independence to compete effectively with peers while in school and in the working world.

Examples of assistive technology devices include:

- Wheelchairs, scooters, walkers, canes, crutches, prosthetic devices, and orthotic devices;
- Computer software and hardware such as voice recognition programs, screen readers and enlargement applications;
- Talking book readers;

- Automatic page-turners, book holders and adapted pencil grips;
- Ramps, automatic door openers, grab bars, wider doorways and adaptive switches. Examples of assistive technology services include:
- Assistive technology evaluations;
- Purchasing or leasing assistive technology devices;
- Selecting, designing, fitting, customizing, adapting, applying, maintaining, repairing or replacing assistive technology devices;
- Coordinating and using other therapies, interventions or services with assistive technology devices, such as those associated with existing education and rehabilitation plans and programs;
- Training or technical assistance for the individual with a disability or, if appropriate, that individual's family;
- Training or technical assistance for professional, employers, or other individuals who provide services to, employ, or are otherwise substantially involved in the major life functions of that person.

EVALUATION

A district level technology committee made up of representatives from each of the buildings, the Technology Support Office, and Curriculum Office will monitor and evaluate of the technology plan. The committee, chaired by the Superintendent of Schools, will meet on a bi-monthly basis to review progress on each of the action plans.

The committee will use a variety of tools to evaluate progress in each of the goal areas. These will include but are not limited to:

- District technology surveys (staff survey done annually)
- Solicited feedback from community participation on planning teams
- Staff Survey Results
- Faculty best practices
- Technology In-service enrollments and exit surveys

Appendix A: Technology Purchase Form

Information Technology Hardware/Software Request
***** Quote Required for processing *****

Name of Requestor:	**Building:** **Funding:** ☐ Building ☐ District ☐ PTO Purchase ☐ Grant
Department:	**Phone Number:**
Desired Installation Date:	**Request Date:**
Primary User: Faculty ☐ Staff ☐ Student ☐ Other ☐	
Type of Purchase (check 1): Desktop ☐ Laptop ☐ Printer ☐ Software ☐ Projector ☐ Whiteboard ☐ Peripheral ☐ Other ☐	**Type of Request (check 1):** New ☐ Renewal ☐ Upgrade ☐ Replacement ☐ Other ☐
Description:	
Location of product installation:	

Quantity Requested:	**Unit Cost:**	**Total Cost:**
How will the product be used and how does it fit into the goals of the current technology plan?		

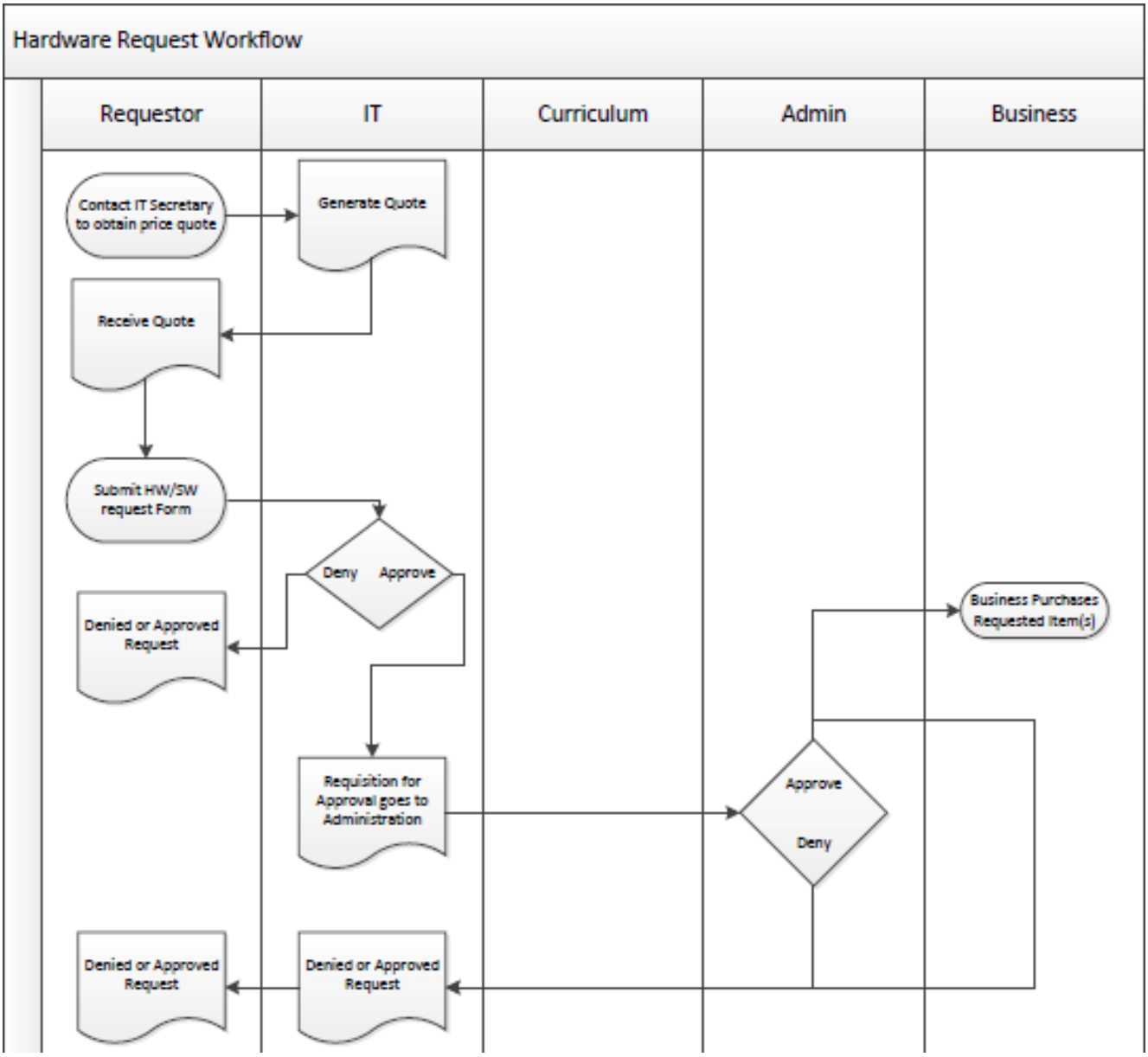
(FOR SOFTWARE REQUESTS)	
License Type: Subscription ☐ One time purchase ☐ Other ☐	**License Term:** 1 year ☐ 2 years ☐ 3 years ☐ Other ☐

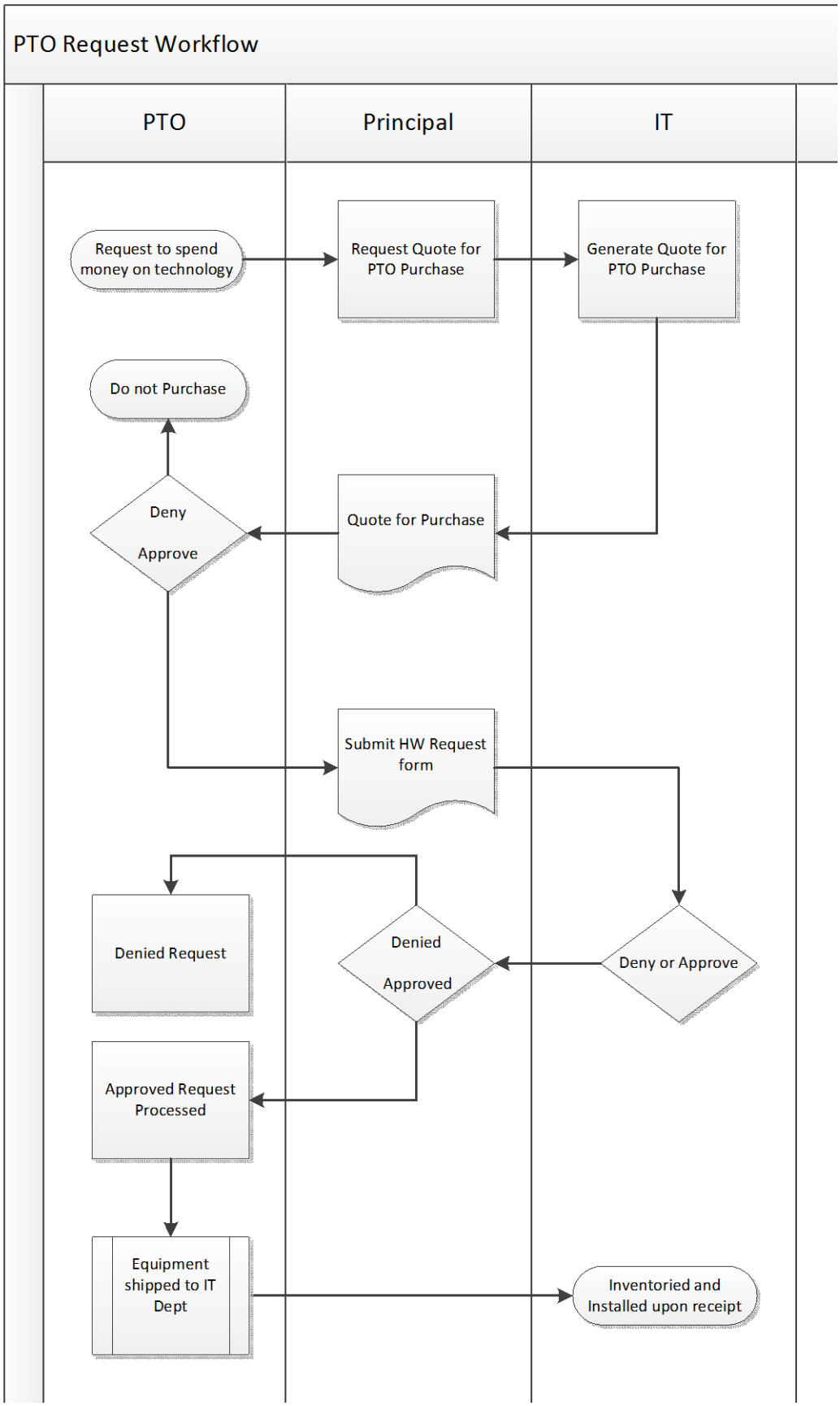
☐ **Approved** ☐ **Denied**

Authorization Signatures

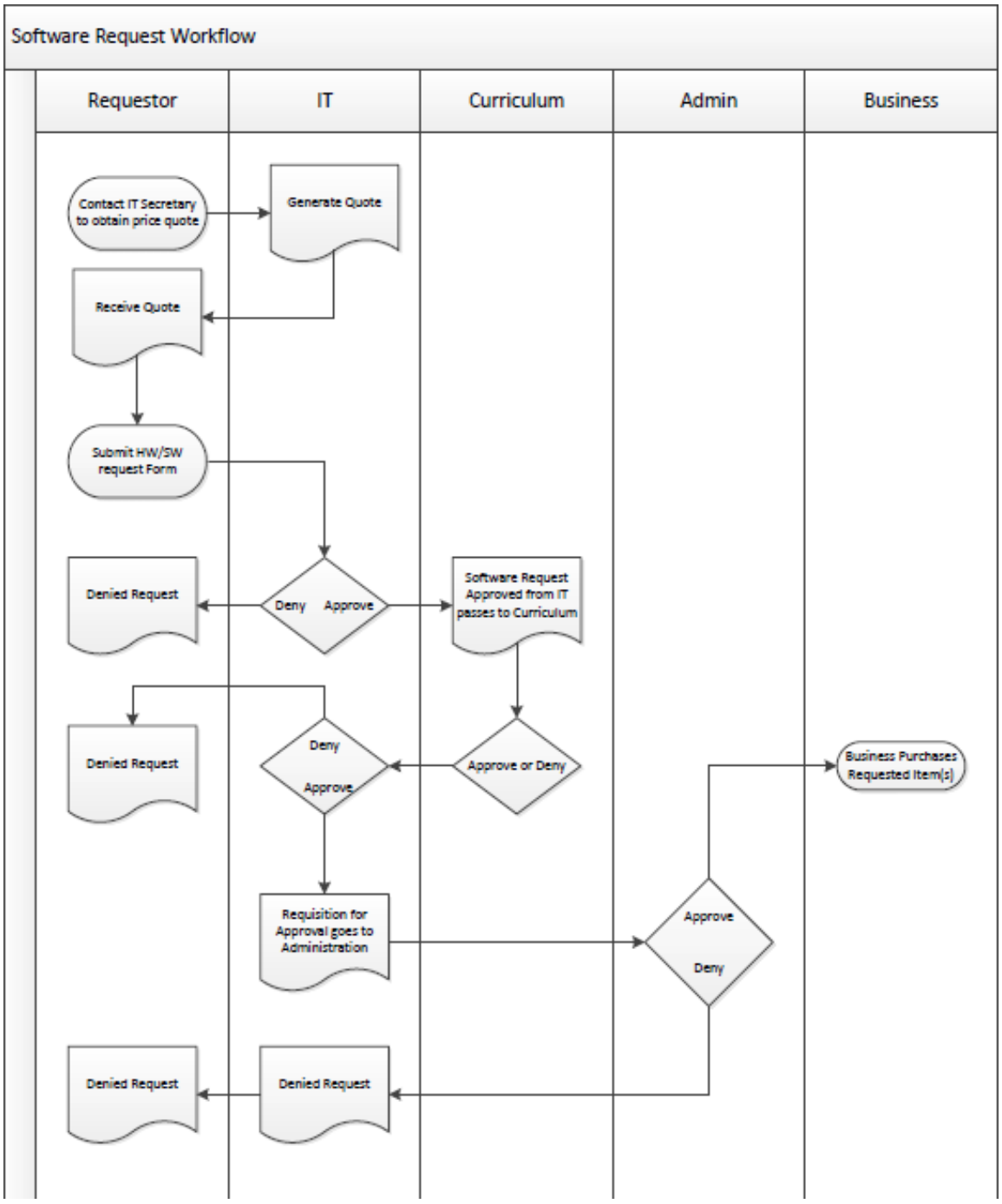
Building Administrator:	Name: Signature:	Date:
Technology:	Name: Signature:	Date:
Curriculum: (Software Requests)	Name: Signature:	Date:
Superintendent or designee:	Name: Signature:	Date:

Appendix B: Hardware Request Workflow




PTO Request Workflow
PTO
Principal
IT
Request to spend money on technology
Request Quote for PTO Purchase
Generate Quote for PTO Purchase
Do not Purchase
Deny
Approve
Quote for Purchase
Submit HW Request form
Denied Request
Denied
Approved
Deny or Approve
Approved Request Processed
Equipment shipped to IT Dept
Inventoried and Installed upon receipt

Appendix C: Software Request Workflow



Appendix D: Acceptable Use of Technology Policy

SUBJECT: ACCEPTABLE USE POLICY AND USE OF EMAIL IN THE DISTRICT

Technology resources are available to students, employees and the Board in the Clarence Central School District. These resources include software delivered via the District local area network, (LAN), as well as the Internet. We are pleased to provide this access to students, employees and Board Members and believe telecommunications and other technological resources offer vast and unique opportunities to the community. The main use of District equipment is for school related purposes. Personal use may be permitted as long as there is no disruption to District operations or mission.

Generally, the same standards for acceptable staff conduct that apply to any aspect of job performance will also apply to use of the District's technology systems. Employees and Board Members are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff.

This policy does not attempt to articulate all required and or acceptable uses of the District's technology systems, nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and uses, as well as prescribed behavior.

District staff and students will also adhere to the laws, policies, and rules governing computers including, but not limited to copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff and student data files and electronic storage areas will remain District property, subject to District control and inspection. The Superintendent or his or her designee may access all such files and communications to ensure system integrity and compliance with requirements of this policy and accompanying regulations. **Staff and students should NOT expect that information stored on the District's computer system will be private. Information may be reviewed without prior notice.**

The use of computers is not only of value to schools but is becoming a necessity in working with students and other aspects of schooling. Various work responsibilities result in access to information sources such as software programs, Internet access and the District's computer network. Access and authorization to information and equipment carry a corresponding responsibility for appropriate use. Access should be primarily for educational and professional activities.

Employees represent the Clarence Central School District and are using a non-private network.

The following is a list of general expectations of all Clarence employees and students.

<u>General Expectations</u>

We expect all employees and students of the Clarence Central School District will:

1) Be familiar with building procedures and rules for computer and Internet use. Employees will abide by expectations contained herein.
2) Be responsible for the security of their computer equipment, files and passwords.

3) Promptly notify their immediate supervisor of security problems.
4) Treat student records with confidentiality and not release or share information except as authorized by Federal and State law.
5) Follow acceptable etiquette, which includes:
   A. Being polite.
   B. Using appropriate language.

We expect that all employees and students of the Clarence Central School District **will not**:

1) Go beyond their authorized access to the District network or other computer equipment or software, including the files or accounts of others.
2) Disrupt or attempt to damage or disrupt any computer system, system performance, or data. This includes the propagation of computer viruses and use of the Internet to make unauthorized entry to any other Internet source.
3) Use District hardware or software to engage in any illegal act.
4) Access or transmit inappropriate items such as pornographic or obscene material, or material that is profane, lewd, rude, inflammatory, or material that contains threatening or disrespectful language.
5) Use potentially damaging, dangerous or disruptive material.
6) Engage in personal or generalized harassment.
7) Transmit false or defamatory information.
8) Be involved in plagiarism.
9) Be involved in malicious activities or downloading or transmitting copyrighted material.
10) Solicit personal information with the intent of using it to cause emotional or physical harm.
11) Use District technology for private business purposes or excessive personal use. No personal use of District technology is permitted that would compromise the District's information technology systems, violate the District's mission, its policies and regulations; violate any State or Federal laws or regulations; interfere with the employee's job requirements or diminish student instructional time.
12) Download and install unauthorized software programs.

When Staff is Working with Students

1) All computer use by students requires supervision.
2) All student Internet use requires supervision.
3) Enforce all aspects of rules governing students.

E-mail and Other User Generated Electronic Files

1) **Employees and students should not have an expectation of privacy.** The Superintendent of Schools (or designee) has the right of access to all e-mail sent or received. In the event of the Clarence Central School District being involved in any legal proceedings, any relevant e-mail recordings (including Internet e-mail), or other electronic files stored on District equipment may be disclosed.

2) Every user is responsible for all e-mail originating from his or her user ID (e-mail address). Forgery or attempted forgery of electronic mail is prohibited. The District e-mail standard is the only allowable e-mail system to be used.

3) Attempts to read, delate, copy or modify the e-mail of other users are prohibited.

Verification of Employee Understanding

All staff must acknowledge and agree to abide by all regulations, organizational policies, guidelines, and procedures that govern computer network, Internet, and information use.

Assumption of Risk

The Clarence Central School District makes no guarantees of any kind, whether expressed or implied, for services provided and is not responsible for any damages suffered while on the system. This includes loss of data and inaccurate or poor-quality information obtained from the system. Furthermore, while use of private devices is acceptable, the owner assumes all the risk for damage, loss or corruption of data.

Web Pages

An exciting innovation in technology is the opportunity for teachers and staff to create teacher Web pages. The Board and the administration encourage the development of Web pages by teachers and staff in order to provide information to parents, students and the community about classroom and student activities as well as instructional resources. To be considered authorized by the Clarence Central School District, Web pages must be developed in accordance with this regulation using resources provided by, and hosted on sites provided by, the Clarence Central School District.

The following guidelines apply to all Web pages developed by Clarence Central School District students and staff and housed within Clarence Central School District's realm of ownership. All information must be in compliance with Clarence Central School District policies, regulations, and Web standards.

Content Integrity

1) All subject matter on the Web pages and their links must relate to:

    A. Curriculum and instruction.

    B. Clarence Central School District authorized activities and services.

    C. Information about the Clarence Central School District or its mission.

2) Safety – Information about students and staff posted on a teacher Web page should be general in nature. Do not use students' full names on the Web. Also, do not give specific locations and times when listing a field trip or activity. Remember that this information is public for anyone to access.

3) Always refer to our organization by using the proper name, the Clarence Central School District.

4) To reduce the possibility of spam, use broken e-mail addresses that do not automatically create a link.

5) Confidential information regarding students, staff, or the organization may not be posted on Web pages.

6) Treat your audience with respect. Avoid any objectionable language and use proper grammar and spelling at all times.

Copyright Information

1) Generally, you cannot post a copy of any copyrighted materials on your website without the copyright owner's permission. Merely acknowledging the source of the copyrighted material is *not* a substitute for obtaining this permission. Materials that may be subject to copyright include photographs, logos, music, videos, cartoons, drawings, paintings, graphs, charts, animation, articles, and other Web pages.

2) Students and staff should assume that any such materials, even if found on the Internet and in the absence of the © symbol or other copyright notice, are subject to copyright.

3) Under certain limited circumstances, teachers are authorized to use portions of copyrighted works in traditional classroom settings under the doctrine of "fair use," without specific permission. However, a copy of a copyrighted work placed by a teacher on a website is less likely to be seen as a "fair use" of that work. Therefore, reliance on a website using "fair use" doctrine should be avoided.

4) Generally, links to copyrighted resources available elsewhere online may be created as long as the link merely directs the user to another site and does not cause a copy of the copyrighted work to be created and stored on Clarence Central School District sites or servers. Include the link disclaimer language. Framing (displaying another site's Web page within our Clarence Central School District Web page design) is not permitted. Your link must cause a separate Web page to appear.

5) Students are the copyright owners of their own work. You must get the written permission of the student, as well as his or her parent, to post a copy of a student's work on your Web page.

Additional Guidelines for the Use of Photos and Images

1) Student photographs, video, audio recordings, or electronic images may be used without prior consent in order to publicize or promote a school district program. If a parent or guardian wishes to refuse permission for the use of a child's photograph, video or audio recording, or electronic images in District publications, media releases, or the District Web site, they must notify the Superintendent of Schools or building principal in writing by September 30 in each academic year.

2) When uploading a file containing an approved photo, please make certain the file name does not list student names (ex.: SallyMae.jpg). If it does, please re-save the photo using another generic description then upload onto the Web. Students' names could be inadvertently shared, accessed as part of the image's code, if not corrected.

3) Photos of individual students or staff are not recommended for security reasons. Group pictures make it harder to identify a specific person in the photo.

4) When using the Clarence Central School District logo, use only the standard logo and do not modify it in any way. When using the logo of another organization (ex.: SkillsUSA), you must get permission in writing first.

5) You may only use images on your Web page with the permission of the copyright owner, unless the image is from a source that specifically grants permission for such use. You cannot scan material from a book and paste it onto your Web page. Handouts created by anyone but you cannot be posted on the Web page. Clip art may be used if from a source that grants permission for such use.

Social Media

The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages technologies to supplement the range of communication and educational services.

For purposes of this Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: Web sites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the school district community, which do not fall within the District's electronic technology network. The definition of District approved password-protected social media tools are those that fall within the District's electronic technology network or which the District had approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access within these internal forums.

However, personal use of these media during District time or on District-owned equipment is prohibited. In addition, employees are encouraged to maintain the highest levels of professionalism. They have responsibilities for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

Applicable Policy and Regulation

All development and use of Web pages and communication tools will be subject to other applicable Clarence Central School District policies and regulations regarding the use and development of instructional materials.

Enforcement

The Superintendent shall be responsible for the enforcement of this policy. Violations of the policy shall be dealt with in accordance with applicable laws, regulations and employee contracts.

Adopted: 6/11/2018

Appendix E: Internet Safety/Content Filtering Policy

SUBJECT: INTERNET SAFETY/INTERNET 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 web sites 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

Adopted: 03/09/2020

Appendix F: Current Inventory

Category	Quantity
Access Point	444
Cart	265
Chromebook	5103
Chromebox	56
Desktop	578
Digital Camera	6
Display	552
Document Camera	350
DVD Player	11
DVD VHS Combo	39
External Hard Drive	3
IA Display	2
IA Projector	337
Label Maker	2
Laptop	2350
LaserDisc Player	4
Monitor	4
Peripheral	63
Phone	696
Printer	276
Projector	96
Scanner	171
Security	6
Server	62
Sound Equipment	34
Storage	1
Switch/Router	220
Tablet	1762
Thin Client	726
UPS	60
VHS Player	16
Video Camera	24
Voice Recorder	44

Appendix G: Privacy And Security For Student Data And Teacher And Principal Data

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d) "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f) "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g) "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

(Continued)

h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) “Eligible student" means a student who is eighteen years or older.

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m) "Parent" means a parent, legal guardian, or person in parental relation to a student.

n) Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

o) "Release" has the same meaning as disclosure or disclose.

p) "Student" means any person attending or seeking to enroll in an educational agency.

q) "Student data" means personally identifiable information from the student records of an educational agency.

r) "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.

s) "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its

(Continued)

responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

t) "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the District will take steps to minimize its collection, processing, and transmission of PII. Additionally, the District will:

a) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

Except as required by law or in the case of educational enrollment data, the District will not report to NYSED the following student data elements:

a) Juvenile delinquency records;

b) Criminal records;

c) Medical and health records; and

d) Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the District.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices

(Continued)

associated with privacy and the security of student data and teacher and principal data.

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer has the power, among others, to:

a) Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and

b) Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the District to perform a privacy impact and security risk assessment.

Data Protection Officer

The District has designated its IT Coordinator to serve as the District's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities. Additionally, some aspects of this role may be outsourced to a provider such as a BOCES, to the extent available.

District Data Privacy and Security Standards

The District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

a) Describe their current cybersecurity posture;

b) Describe their target state for cybersecurity;

c) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

(Continued)

d) Assess progress toward the target state; and

e) Communicate among internal and external stakeholders about cybersecurity risk.

The District will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:

    1. Improve academic achievement;

    2. Empower parents and students with information; and/or

    3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

c) The District affords all protections under FERPA and the Individuals with Disabilities

Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-Party Contractors

District Responsibilities

The District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

In addition, the District will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the District.

The third-party contractor's data privacy and security plan must, at a minimum:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with District policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

(Continued)

d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;

e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;

g) Describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the District under which the third-party contractor will receive student data or teacher or principal data from the District, is required to:

a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b) Comply with District policy and Education Law Section 2-d and its implementing regulations;

c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the District; or

2. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

(Continued)

f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g) Use encryption to protect PII in its custody while in motion or at rest; and

h) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Cooperative Educational Services through a BOCES

The District may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from the District under all circumstances.

For example, the District may not need its own contract or agreement where:

a) It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and

b) That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the District's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from the District is received by a third-party contractor pursuant to a CoSer, the District will consult with the BOCES to, among other things:

a) Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the District's use of a third-party contractor's product or service under a particular CoSer;

b) Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;

c) Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from the District pursuant to a BOCES contract; and

(Continued)

d) Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the District receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the District pursuant to a BOCES contract.

Click-Wrap Agreements

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

District staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Privacy Officer or designee.

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The District's Bill of Rights will state in clear and plain English terms that:

a) A student's PII cannot be sold or released for any commercial purposes;

b) Parents have the right to inspect and review the complete contents of their child's education record;

c) State and federal laws protect the confidentiality of PII, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred;

d) A complete list of all student data elements collected by the state is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234; and

(Continued)

e) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure.

The Bill of Rights will also include supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District. The supplemental information must be developed by the District and include the following information:

a) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

b) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

c) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

d) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

e) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

f) Address how the data will be protected using encryption while in motion and at rest.

The District will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the District under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the District in a manner prescribed by the District.

(Continued)

The District will ensure that only authorized individuals are able to inspect and review student data. To that end, the District will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the District and not to a third-party contractor. The District may require that requests to inspect and review education records be made in writing.

The District will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the District through its annual FERPA notice. A notice separate from the District's annual FERPA notice is not required.

The District will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The District may provide the records to a parent or eligible student electronically, if the parent consents. The District must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the District about breaches or unauthorized releases of student data and/or teacher or principal data:

a) All complaints must be submitted to the District's Data Protection Officer in writing.

b) Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) Following the investigation of a submitted complaint, the District will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the District.

d) If the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District will provide the individual who

(Continued)

filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other District staff.

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Reporting a Breach or Unauthorized Release

The District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal

(Continued)

data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, District policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than 30 days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

a) Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years;

b) Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years;

c) Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or

d) Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

The District will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the District or the receipt of

(Continued)

a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the District will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

b) A description of the types of PII affected;

c) An estimate of the number of records affected;

d) A brief description of the District's investigation or plan to investigate; and

e) Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the District for the full cost of this notification.

Annual Data Privacy and Security Training

The District will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

Notification of Policy

The District will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121

Adopted: 4/6/2020