DANSVILLE CENTRAL SCHOOL

Leaders in Technology for Learning

2018-2021

Technology Plan

Updated September 22, 2015
June 2016
June 2017
June 2018

TABLE OF CONTENTS

Dansville Vision & Mission Statements

DCSD Vision: DCS students will exemplify the drive, capability and compassion to achieve their full potential while contributing to our evolving local and global communities.

DCSD Mission: The Dansville school community is committed to providing a high quality education for all students of the school district to;

- Educate each student to his/her fullest potential;
- Prepare all students for the world of work and/or further formal education;
- Promote the development of responsibility, mutual respect, and self discipline in learning and personal behavior;
- Challenge and encourage students to become lifelong learners and creative, critical thinkers toward a better world.

Technology Mission Statement

The mission of Dansville Central School District Technology Plan is to support the creation of a collaborative learning environment for all, in which our students can achieve their full potential and contribute to our evolving local and global communities. This environment will enable and support students and teachers to implement transformative uses of technology while enhancing students' engagement with content and promoting the development of self-directed and life-long learners. Students will transition from consumers of information to creative producers and owners of knowledge. Specifically we aspire for our students to be:

- ★ Critical thinkers who see information and critically analyze and evaluate
- ★ *Problem solvers and decision makers who can persevere*
- ★ *Creative and effective users of productivity tools*
- ★ *Communicators, collaborators, publishers and producers*
- ★ *Informed, responsible and contributing citizens*

To ensure DCS students exemplify the drive capability and compassion to achieve their full potential, we are committed to further developing collaborative professional learning communities based on integrative professional development for teachers, enhancing classroom environments implementing high-quality instruction, assessment and learning through the integration of technology and curriculum.

The Board of Education, district staff and community members will all play a key role in the development and support of of effective and high quality 21st Century educational experiences.

District Goals 2018-2019

1. Promote STEM by integrating instructional technology with curriculum, pedagogy, and assessment to foster critical thinking and real world problem solving.
2. Align District Instructional Technology Curriculum to ISTE Standards and develop grade level guidelines
3. Create a positive school culture that supports safe and responsible technology use through continued and enhanced Digital Citizenship curriculum PK-12.
4. Maintain and support DCS PK-12 1:1 device environment, robust network, and all supporting equipment and software

District Beliefs:

The Dansville School District believes that a digitally rich curriculum, instruction, and assessment supports the 7 Habits goal of empowering students to adapt to our rapidly changing society, and seeks to ensure that all students and staff be able to create, access, exchange, and analyze information from electronic sources.

Digitally rich curriculum is essential to:

- Solving complex problems
- Working collaboratively, locally, nationally and globally
- Communicating effectively
- Preparing students for college acceptance or for alternative paths to workplace readiness
- Achieving NYS Next Gen Learning and Content Standards aligned instruction
- Student self-directed learning
- Authentic learning in the context of today's digital society
- Assessing instructional efficacy both formative and summative
- Data analysis
- Improving student academic achievement through increased participation and engagement
- Improving student motivation and learning
- Providing access to a wide array of information, and ensure critical evaluation of the same
- Accommodating different curriculum needs and different learning styles

- Assisting staff with record keeping, including but not limited to student grades and records, and progress monitoring

District Commitments:

The District Administration and Technology support are committed to:

1. Students having access to information and technologies needed to function as productive members of the 21st century.
2. Supporting teachers and staff in developing and using relevant technologies to prepare curriculum and instruction.
3. Providing ongoing Professional Learning as well as classroom support.
4. Creating/enhancing Learning Environments which include personalized approaches to teaching and collaborative work.
5. Creating and actively carrying out a technology plan to guide the integration of computer technology and to regularly seek feedback, and update this plan.
6. Provide district-wide opportunities for continual technological education for students, parents, and community.
7. Ensure the continuity and coordination of acquisition, application, replacement, and maintenance of changing technology
8. Improve student achievement.
9. Encourage, Plan, and support district and building efforts to promote and enforce responsible technology use by entire school community by embracing and supporting Digital Citizenship programs and instruction

District Action Plan 2018 - 2019

Goal 1: Promote STEM by integrating instructional technology with curriculum, pedagogy, and assessment to foster critical thinking and real world problem solving.

Goal 1 Action Plans: Promote and support Instruction across the district that supports Personalized Digital Learning. Personalized learning is a student-centered approach designed to help all students develop a set of skills collectively known as the deeper learning competencies. These skills include thinking critically, using knowledge and information to solve complex problems, working collaboratively, communicating effectively, learning how to learn, and developing academic mindsets:

Digitally rich Curriculum, Instruction and assessment for Teachers / Staff Action Plans:

1. Professional learning to sustain and expand teacher and student learning through instructional technology
    - Appy Hours - (Genius Hour) - develop a cadre of teachers to facilitate sessions for other teachers on curricular topics to include digitally rich curriculum, instruction, and assessment.
    - Kagan Cooperative Learning
        - Professional Development sessions - August 21 & 22
        - Follow up with Appy Hours on Kagan Structures to support digitally rich curriculum, instruction and assessment.
    - 7 Habits Empowering Instruction
        - Professional Development sessions - entire staff - October 5
        - Coaching - Lighthouse Teams - October 2018
        - Coaching with teams - second semester
    - Units of Study in Reading and Writing -
        - Writing Conference - August 15 & 16
        - Follow up PD at grade levels - collaborative writing, lab sites
        - Coaching with Reading & Writing Specialist - rotate through grade levels
    - Other training available to staff to support digitally rich curriculum, instruction and assessment: BOCES Training, NYSCATE, EdTech, Instructional Technology Coaching - approval through Curriculum office in alignment with district goals and PD plan
2. Collaborate and Plan for Equitable Technology Support - Ensure equitable access to digitally rich curriculum, assessment, and instruction with assistive technology for students with disabilities and English language learners
3.

Instructional Technology for Students Action Plans

1. PK-12 Technology Curriculum
    a. Elementary - Library Media Specialists provide digitally rich curriculum in coding and digital citizenship. Technology TAs provide digitally rich curriculum in technology skills
        i. 2018-19 Coding and Digital Citizenship - audit and align
        ii. 2019-20 Expand offerings
    b. Secondary - HS Course offerings to expand in STEM both college bound students and skilled trades
        i. CFM
        ii. FACs
        iii. Push-In Digital Citizenship

1. Above 3: 2018-19 work with CFM and FACs teachers to incorporate more coding and tech skills into curriculum
2. 2019-2020 - offer new courses as well as required CFM and FACs
3.

iv. Internships, in partnership with community businesses and other educational partners

2. Enrichment
    a. GETT Summer Camp SETT/GETT, and continues to evolve into HS Technology Club/ Robotics
    b. Support of and Expansion of partnerships such Fenn Institute, Tech Wars, Entrepreneur Clubs, Robotics, etc.

BUDGET:

- **Professional Development (Part of Curriculum and Instruction) - $92,000**

TIMELINE:

- **Ongoing for 2018-2021 with budget 92,000 - 172,000 per year**

Goal 2: Align District Instructional Technology Curriculum to ISTE Standards and develop grade level guidelines

1. Convene and Develop STEM Steering Committee to guide district to enhanced STEM curriculum and instruction for college and career readiness PK - 12
    - In our 5th year since digital conversion, we will conduct a STEM Audit with consultant
    - With input from Audit, align and develop instructional technology classes both internally and community college partnerships.
    - The STEM Steering Group will explore and advocate for expansion of instructional technology, STEM courses and enrichment opportunities as well as partnerships with other community and educational partners
        - 2019 - pilot HS tech courses, P-Tech Academy
        - 2020 - expand STEM in HS and elementary
    - NSF - Noyce Master Teaching Fellows Program
        - 2018 - select fellows
        - 2020 - PD provided by Fellow(s) to expand STEM capacity of all teachers
2. Refine and Align Instructional Technology Curriculum PK - 12
    - Update and align instructional technology curriculum for students so all are instructed in basic technology skills, coding, study skills, and digital citizenship.
    - ISTE Standards for Students - align to Empowering Instruction and develop Grade Level learning standards for students

- Identify critical Instructional Technology Curriculum to be infused in digitally rich curriculum, instruction and assessment in each grade level, FACs, and CFM
- Ensuring equitable access to curriculum, instruction, and assessment with technology and assistive technology as appropriate to increase student engagement and learning for students with disabilities and English Language Learners
- Computer Technology Trainers are available to assist in such instruction in the
- Library Media Specialists in all buildings will provide ongoing instruction at all grade levels in collaboration with classroom teachers.

BUDGET:

- **Professional Development -** In house, staff salaries
  - Conferences - curriculum budget

Goal 3: Create a positive school culture that supports safe and responsible technology use through continued and enhanced Digital Citizenship curriculum PK-12.

Digital Citizenship - Being a good digital citizen is more than knowing your way around the web. It's about connecting and collaborating in ways you didn't even know were possible. The DCS Digital Citizenship Curriculum is based on Common Sense

Digital Citizenship is a concept which helps teachers, technology leaders and parents to understand what students/children/technology users should know to use technology appropriately. Digital Citizenship is more than just a teaching tool; it is a way to prepare students/technology users for a society full of technology, while guarding against the destructive side of technology including addictive use, and unsafe practices. Digital citizenship is the norms of appropriate, responsible technology use. Too often we are seeing students as well as adults misusing and abusing technology but not sure what to do. The issue is more than what users do not know but what is considered appropriate technology usage. In 2016-2017, we focused on infusing awareness of what Digital Citizenship entails, informing students on many occasions, supporting staff in embedding this into instruction and routines, and aligning with our adoption of the Leader in Me Curriculum. In 2017-2018 we continued these efforts in PK - 6 with library, counselors, and classroom curriculum. We also provided appropriate digital citizenship integration through push-in programs in classrooms. At the secondary level, assemblies for students continued and the library/media specialist and tech PD support pushed into classrooms to offer instruction in Digital Footprint, Organizing Drive, Authentic Research, and developing a Digital Portfolio. In 2018-19 we will align our Digital Citizenship curriculum PK-12 to ensure we are building a coherent body of knowledge for our students. We will continue our push in at 7-12 with the following topics: and we will infuse parts of the curriculum into FACs and CFM

Our Digital Citizenship Curriculum focuses on 8 Subjects in the Common Sense Media scope and sequence:

1. Internet Safety
2. Digital Footprints & Reputation
3. Privacy & Security
4. Self Image & Identity
5. Relationships & Communication
6. Information Literacy
7. Cyberbullying & Digital Drama
8. Creative Credit & Copyright

Digital Citizenship Action Plans:

1. Refine and Align Instructional Technology Curriculum PK - 12
    - Update and align instructional technology curriculum for students so all are instructed in digital citizenship
2. Development of push-in program in Digital Citizenship
3. Library Media Specialists support Direct instruction in Digital Citizenship
4. Presentations to Students, Student Forums, and Student Surveys to develop 2 way communication about digital standards.

BUDGET: In house salaries partially covered in Title IIA - $82,000
TIMELINES: Ongoing

Goal 4 - Maintain and support DCS PK-12 1:1 device environment, robust network, and all supporting equipment and software

Action Plan - Ongoing Support of Instructional Technology

- Plan for professional Learning and Follow up
    - Annually - budget listed under goal 1
- Advise superintendent on SMART Bond Act and long term funding of 1:1 initiative to continue instructional technology to support teaching and learning.
- Ensure Utilization of technology, especially district-wide wireless network to enhance district communication internally and externally, record keeping, data availability and efficiency. Deploying these systems is intended to give teachers/administrators tools to help meet the increasing demands of data management
- Maintain a single district-wide student records database solution (SchoolTool) with web access for students, parents and teachers, and Food Service and Transportation databases. Ongoing annual Training in School Tool (link to iReady through Clever) and other district technology for new employees. Wayne-Finger Lakes Edutech provides

ongoing support.

- Continue streamlining collaboration software to promote district-wide efficiency with instructional technology support (G-Suite, Google Drive, iReady Student Assessments, Progress monitoring and instruction, and Data Analysis, eDoctrina Assessment development and data analysis) .
- District Communication - coordination between administrative team and Data Coordinator which supports a single student records database manager responsible for data integrity, district training and data warehouse responsibility.
- Monitoring of Website, Blackboard to promote Expanded and updated communication with school community.
- Ensure needs of students with disabilities and ESL students are supported with technology as necessary to allow equitable access to curriculum, instruction and assessment
- Use Blackboard Connect, website, and DCS App to allow customized voice messages to be efficiently delivered to DCS students, staff and parents.
- Maintain funding for replacement of devices according to 1:1 Roadmap (See Appendix E) with SMART Bond funds through 2022 and transitioning back to EduTech leases slowly beginning in 2021

BUDGET:

- Professional Development - provided for in Goal 1
- EduTech Support: $631,000
- Computer Equipment: $ 30,000
- Computer Repairs $ 12,587
- Computer Supplies $ 15,000
- Computer Parts $ 30,000
- Software $ 23,000

SMART BOND FUNDING

- 1:1 Roadmap annual expenses $175,000
- Security Costs 2018-19 $ 80,000

Evaluation Process

Teacher/student feedback will be solicited continuously in an informal manner and once in a school year in a formal way through surveys. The Technology Committee will review and make adjustments. Teachers/administrators will review student performance to evaluate effectiveness of software applications and hardware in achieving goals.

Budget

The district technology budget provides funds to seamlessly integrate effective instructional technology designed to enhance student engagement, transform teaching and increase student learning. The budget and the NYS SMART Bond Act funds allocated to Dansville provide

resources to cyclically replace computers (see 1:1 Road Map in appendices below) and software in classrooms, labs, and libraries based on an annually updated projection plans prepared by the Director of Technology, in conjunction with the Tech Steering Committee. This projection also includes replacement of servers/network hardware and software necessary to maintain the district infrastructure to a high standard. Additional funds are annually budgeted for specific hardware/software requests from end users. Professional Learning budget is part of the district Curriculum and PD funds.

The “SchoolTool” student records database support will be funded through a Wayne-Finger Lakes Administration SAA. Internet hosting/development are funded through a Wayne-Finger Lakes SAA. The Blackboard Connect system will be funded through a Wayne-Finger Lakes SAA. Some Hardware purchases will be funded through Technology Budget, and some through SMART Bond Act reimbursements. Any additional software would be funded through the district software budget and/or the Wayne-Finger Lakes Administration SAA.

BUDGET - Long Range Planning:

Priority Planning for SMART Bond Act is developed collaboratively between administration and faculty. The district has an SSIP plan aligned with this Technology plan, both of which are approved by NYSED.

Continued annual budget funding for software, hardware and repairs as well as professional development

DCS Computer Technology Infrastructure

1. Windows 10/Chromebooks. A common desktop interface lets our users spend more time working. Ease in creating multimedia presentations attracts greater student/faculty interest in employing technology in the classroom. Desktop systems are scheduled for cyclical replacement to ensure users are trained on modern equipment and to minimize down time due to hardware failure.

2. Network Protocol TCP/IP. This standard ensures vendor interoperability and fault tolerant, efficient communication between devices.

3. Hardware Vendor(s) hardware is purchased from state-bid approved vendors offering tier

one equipment. By purchasing reliable, low-cost hardware we are able to offer more resources to our learning communities. Low down time due to quality components and ready parts availability ensures more technology-based learning time.

4. Local Network Infrastructure - inter-building switched fiber optic 10 gigabit backbone with gigabit copper connections to servers/desktops. The fiber connection to our Middle School and Transportation office is leased through Time-Warner. The fiber connection to our remote Middle School offers reliable, high-speed access to campus resources while saving on hardware costs. Likewise, the fiber connection to our remote transportation department allows high-speed access to a web-based transportation routing application and the student records database. The wireless infrastructure consists of Meru APs running 802.11ac with at least one AP in each classroom and multiple APs in large instruction locations.

5. Wide-Area Network Infrastructure - 600 mbps fiber (as of July 1, 2018), (Time-Warner contracted through Edutech). The move to our new fiber connection has made streaming video, audio, and distance learning over the internet a reality. Students and teachers benefit from rapid internet searching and downloads allowing more time spent learning rather than waiting for information on congested links. The expanded resources offered via the internet promote advanced student research and learning opportunities to worldwide resources. Remote access to school resources is available through Edutech' s Cisco VPN solution. This allows teachers and administrators the flexibility to work from home. Increased, stable bandwidth allows us to run more web-based applications which reduce our local hardware and support costs.

6. Internet Service Provider - Spectrum, contracted through Edutech ,provides reliable, managed services resulting in high up time.

7. District Web Site - In 2017 the district transitioned to a new website with Blackboard. This includes a new mass communication system and an app. Emphasis on ease of communication with community, social media, and mobile devices, the new website will enhance communication and collaboration with our community. Teachers can create web pages on the new website. Projects requiring student-authored web pages, particularly with Google Sites teach students valuable 21st century communication methods and inspire learning and creativity. The district internet web site (http://www.dansvillecsd.org/) provides a wealth of school information to the community, and enhanced communication, contact with social media and a district app to allow greater communication and access to district info. Lunch menus and sports schedules will be readily available on SMARTphones with just a few clicks. The App provides means to communicate directly with school officials.

8. Email Services - G-Suite Apps for Education. Message archiving for 10 years will deployed via Google Vault.

9. Internet Filter - GoGuardian for Student Chromebooks and iBoss for staff Chromebooks and Windows based PCs, both contracted through Edutech. With a district-controlled internet filter

we are able to customize the configuration to allow teachers the freedom they need to efficiently search the internet for learning resources, while preventing students from visiting inappropriate sites.

10. Wireless Voice/Data Services - District administrators are able to work more effectively by being able to communicate anytime, anyplace via voice or email.

11. Office Automation - Microsoft Office 2016, G-Suite for Education.

12. Desktop Platform - Windows 10 Professional

13. Wireless Devices - Chromebooks and iPads/Androids

14. SPAM Filter - Integrated into Google Apps for Education.

Internet Safety Plan

Introduction

It is the policy of the Dansville Central School District that all employees and students within the Dansville Central School District shall adhere to the Dansville Central School District Acceptable Use Policy (AUP). Acceptable Use Agreement is required each time staff, students, or guests log on to any of our networks. Compliance with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(n)].

Definition

Key terms are as defined in the Children's Internet Protection Act.*

Access to Inappropriate Material

As per the Dansville Central School District's AUP, filtering software is in place to block or filter the internet and other forms of electronic communication.

Specifically, as required by the Children's Internet Protection Act, blocking applies to all written as well as visual depictions of material deemed obscene or child pornography, and to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

As per the Dansville Central School District's AUP, all forms of electronic communication are blocked by filtering software for student users.

The Dansville Central School District's AUP strictly forbids inappropriate network usage as outlined within the illegal activities section.

Education, Supervision and Monitoring

It shall be the responsibility of all staff members of the Dansville Central School District to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Coordinator or designated representatives.

Adoption

The Dansville Central School District School Board has approved and adopted the Internet Safety Policy as part of the District Technology Plan.

Addendum

APPENDIX A: ISTE Standards for Students
APPENDIX B: ISTE Standards for Teachers
APPENDIX C: ISTE Standards for Administrators
APPENDIX D: Technology Use Guide
APPENDIX E: 1:1 Road Map
APPENDIX F: Acceptable Use Policy (AUP)
APPENDIX G: FERPA Notification
APPENDIX H: Parent Bill of Rights
APPENDIX I: Code Of Conduct Documents
APPENDIX J: Technology Committee Members

Appendix A: ISTE Standards for Students

Technology Foundation Standards for All Students

The technology foundation standards for students are divided into six broad categories. Standards within each category are to be introduced, reinforced, and mastered by students. These categories provide a framework for linking performance indicators within the Profiles for Technology Literate Students to the standards. Teachers can use these standards and profiles as guidelines for planning technology-based activities in which students achieve success in learning, communication, and life skills.

1. Creativity and innovation Students demonstrate creative thinking, construct knowledge, and develop innovative products and processes using technology
    a. Apply existing knowledge to generate new ideas, products, or processes
    b. Create original works as a means of personal or group expression
    c. Use models and simulations to explore complex systems and issues
    d. Identify trends and forecast possibilities
2. Communication and collaboration Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others.
    a. Interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media
    b. Communicate information and ideas effectively to multiple audiences using a variety of media and formats
    c. Develop cultural understanding and global awareness by engaging with learners of other cultures
    d. Contribute to project teams to produce original works or solve problems
3. Research and information fluency Students apply digital tools to gather, evaluate, and use information.
    a. Plan strategies to guide inquiry
    b. Locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media
    c. Evaluate and select information sources and digital tools based on the appropriateness to specific tasks
    d. Process data and report results
4. Critical thinking, problem solving, and decision making Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources.
    a. Identify and define authentic problems and significant questions for investigation
    b. Plan and manage activities to develop a solution or complete a project
    c. Collect and analyze data to identify solutions and/or make informed decisions
    d. Use multiple processes and diverse perspectives to explore alternative solutions
5. Digital citizenship Students understand human, cultural, and societal issues related to

technology and practice legal and ethical behavior.

a. Advocate and practice safe, legal, and responsible use of information and technology
b. Exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity
c. Demonstrate personal responsibility for lifelong learning
d. Exhibit leadership for digital citizenship

6. Technology operations and concepts Students demonstrate a sound understanding of technology concepts, systems, and operations.
    a. Understand and use technology systems
    b. Select and use applications effectively and productively
    c. Troubleshoot systems and applications
    d. Transfer current knowledge to learning of new technologies

Appendix B: ISTE Standards for Teachers

DCS Seeks to continuously improve teacher technology skills as provided for in ISTE Standards for Teachers through ongoing professional development as outlined in this document.

Educational Technology Standards and Performance Indicators for All Teachers

Effective teachers model and apply the ISTE Standards for Students (Standards•S) as they design, implement, and assess learning experiences to engage students and improve learning; enrich professional practice; and provide positive models for students, colleagues, and the community. All teachers should meet the following standards and performance indicators.

1. Facilitate and inspire student learning and creativity Teachers use their knowledge of subject matter, teaching and learning, and technology to facilitate experiences that advance student learning, creativity, and innovation in both face-to-face and virtual environments.
    a. Promote, support, and model creative and innovative thinking and inventiveness
    b. Engage students in exploring real-world issues and solving authentic problems using digital tools and resources
    c. Promote student reflection using collaborative tools to reveal and clarify students' conceptual understanding and thinking, planning, and creative processes
    d. Model collaborative knowledge construction by engaging in learning with students, colleagues, and others in face-to-face and virtual environments
2. Design and develop digital age learning experiences and assessments Teachers design, develop, and evaluate authentic learning experiences and assessments incorporating contemporary tools and resources to maximize content learning in context and to develop the knowledge, skills, and attitudes identified in the Standards•S.
    a. Design or adapt relevant learning experiences that incorporate digital tools and resources to promote student learning and creativity

    b. Develop technology-enriched learning environments that enable all students to pursue their individual curiosities and become active participants in setting their own educational goals, managing their own learning, and assessing their own progress
    c. Customize and personalize learning activities to address students' diverse learning styles, working strategies, and abilities using digital tools and resources
    d. Provide students with multiple and varied formative and summative assessments aligned with content and technology standards, and use resulting data to inform learning and teaching
3. Model digital age work and learning Teachers exhibit knowledge, skills, and work processes representative of an innovative professional in a global and digital society.
    a. Demonstrate fluency in technology systems and the transfer of current knowledge to new technologies and situations
    b. Collaborate with students, peers, parents, and community members using digital tools and resources to support student success and innovation
    c. Communicate relevant information and ideas effectively to students, parents, and peers using a variety of digital age media and formats
    d. Model and facilitate effective use of current and emerging digital tools to locate, analyze, evaluate, and use information resources to support research and learning
4. Promote and model digital citizenship and responsibility Teachers understand local and global societal issues and responsibilities in an evolving digital culture and exhibit legal and ethical behavior in their professional practices.
    a. Advocate, model, and teach safe, legal, and ethical use of digital information and technology, including respect for copyright, intellectual property, and the appropriate documentation of sources
    b. Address the diverse needs of all learners by using learner-centered strategies providing equitable access to appropriate digital tools and resources
    c. Promote and model digital etiquette and responsible social interactions related to the use of technology and information
    d. Develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital age communication and collaboration tools
5. Engage in professional growth and leadership Teachers continuously improve their professional practice, model lifelong learning, and exhibit leadership in their school and professional community by promoting and demonstrating the effective use of digital tools and resources.
    a. Participate in local and global learning communities to explore creative applications of technology to improve student learning
    b. Exhibit leadership by demonstrating a vision of technology infusion, participating in shared decision making and community building, and developing the leadership and technology skills of others
    c. Evaluate and reflect on current research and professional practice on a regular

basis to make effective use of existing and emerging digital tools and resources in support of student learning

d. Contribute to the effectiveness, vitality, and self-renewal of the teaching profession and of their school and community

Appendix C: ISTE Standards for Administrators

DCS Seeks to continuously improve administrator technology skills as provided for in Nets for Administrators through ongoing professional development as outlined in this document.

Educational Technology Standards and Performance Indicators for Administrators

1. Visionary leadership Educational Administrators inspire and lead development and implementation of a shared vision for comprehensive integration of technology to promote excellence and support transformation throughout the organization.
    a. Inspire and facilitate among all stakeholders a shared vision of purposeful change that maximizes use of digital-age resources to meet and exceed learning goals, support effective instructional practice, and maximize performance of district and school leaders
    b. Engage in an ongoing process to develop, implement, and communicate technology-infused strategic plans aligned with a shared vision
    c. Advocate on local, state and national levels for policies, programs, and funding to support implementation of a technology-infused vision and strategic plan

2. Digital age learning culture Educational Administrators create, promote, and sustain a dynamic, digital-age learning culture that provides a rigorous, relevant, and engaging education for all students.
    a. Ensure instructional innovation focused on continuous improvement of digital-age learning
    b. Model and promote the frequent and effective use of technology for learning
    c. Provide learner-centered environments equipped with technology and learning resources to meet the individual, diverse needs of all learners
    d. Ensure effective practice in the study of technology and its infusion across the curriculum
    e. Promote and participate in local, national, and global learning communities that stimulate innovation, creativity, and digital age collaboration

3. Excellence in professional practice Educational Administrators promote an environment of professional learning and innovation that empowers educators to enhance student learning through the infusion of contemporary technologies and digital resources.
    a. Allocate time, resources, and access to ensure ongoing professional growth in technology fluency and integration

b. Facilitate and participate in learning communities that stimulate, nurture and support administrators, faculty, and staff in the study and use of technology
c. Promote and model effective communication and collaboration among stakeholders using digital age tools
d. Stay abreast of educational research and emerging trends regarding effective use of technology and encourage evaluation of new technologies for their potential to improve student learning

4. Systemic improvement Educational Administrators provide digital age leadership and management to continuously improve the organization through the effective use of information and technology resources.
    a. Lead purposeful change to maximize the achievement of learning goals through the appropriate use of technology and media-rich resources
    b. Collaborate to establish metrics, collect and analyze data, interpret results, and share findings to improve staff performance and student learning
    c. Recruit and retain highly competent personnel who use technology creatively and proficiently to advance academic and operational goals
    d. Establish and leverage strategic partnerships to support systemic improvement
    e. Establish and maintain a robust infrastructure for technology including integrated, interoperable technology systems to support management, operations, teaching, and learning

5. Digital citizenship Educational Administrators model and facilitate understanding of social, ethical and legal issues and responsibilities related to an evolving digital culture.
    a. Ensure equitable access to appropriate digital tools and resources to meet the needs of all learners
    b. Promote, model and establish policies for safe, legal, and ethical use of digital information and technology
    c. Promote and model responsible social interactions related to the use of technology and information
    d. Model and facilitate the development of a shared cultural understanding and involvement in global issues through the use of contemporary communication and collaboration tools

Appendix D: Technology Use Guide

Dansville District Technology Use Guide

Access to the Dansville District Technology resources is a privilege and not a right. Each employee, student and/or parent will be required to follow the district's Acceptable Use Policy (below Appendix F)

Receipt of Chromebook

Chromebooks will be distributed. Parents, guardians, and students are made aware of the District's Acceptable Use Policy. This policy outlines procedures and policies for families, staff, and students.

Chromebooks will be collected at the end of each school year. Instructions will be given at a later date.

Students leaving the district must return Chromebooks to the Technology Department. Any chromebook that is not returned will be considered stolen property, after multiple attempts to collect.

Student Owned Devices

Student devices are not supported for instructional purposes.

Appropriate Use

The Dansville Central School District views the use of electronic resources as central to the delivery of its educational program and expects that all students will use electronic resources as an essential part of their learning experiences. It is the policy of the Dansville Central School District to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities.

General Guidelines

- Use of the Chromebook and other electronic devices issued by the district must support education.
- All regulations are in effect before, during, and after school hours, for all computers.
- Headphones may be used at the discretion of the teacher
- Students should not connect Chromebooks or other electronic devices issued by the district to Ethernet jacks at school.
- Chromebook of other electronic devices issued by the district use in study halls/detention is for instructional purposes only.
- Messaging is only allowed during school hours with permission from the teacher. Permission will be given only for messaging that is useful in school assignments and must be related to school assignments.

Monitored Use

- All files stored on the system are the property of the district and are subject to regular review and monitoring.
- DCSD reviews and monitors all activity on the computers/network for responsible use.
- Internet history and e-mail checks will occur at least once a month. They will be random and unannounced.
- Students must retain at least 2 weeks of Internet history.
- Students must retain full email folders (inbox, outbox, sent, deleted etc.)
- Changing computer settings is not allowed.

General Reminders: In School

1. All student use of computers or other technology should be in support of their education.
2. All use of technology must comply with the ***District Policy as well as the Acceptable Use Policy***.
3. Student in whose name a Chromebook or other electronic device is issued will be responsible at all times for its appropriate use.
4. All use of the Internet must comply with district guidelines. Log files are maintained on each computer with a detailed history of all sites accessed. These files may be reviewed periodically.
5. All Chromebooks and other district devices contain a remote content filter for use at school. However, no filter is as reliable as a teacher.
6. Teachers are responsible for monitoring student Chromebook and other district issued electronic devices use at school, especially Internet access.
7. Students who identify or know about a security problem are expected to convey the details to their teacher without discussing it with other students.
8. Students are expected to notify a staff member immediately if they come across information, images or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.
9. All users are expected to comply with existing copyright laws.
10. Students may only log in under their assigned user name. Students may not share their password with other students.
11. Students are responsible for charging the Chromebook or other district issued electronic device battery at home (if taken home) or school (if not taken home) each day.
12. Students are expected to care for the Chromebooks or other district issued device. If a Chromebook or other district issued device is deemed to be intentionally damaged by a student, the student may be subject to discipline and the student/parent will also be responsible for the full cost of the Chromebook or other district issued electronic device repair.
13. Students are expected to report any damage to the computers immediately. Spot inspections of Chromebooks or other district issued electronic devices may occur regularly. Students who do not report damage or abuse will be subject to both fines and discipline.
14. Students are expected to keep track of all equipment issued to them. If components are lost, the student/parent will be responsible for the full cost of replacement.
15. Students may not loan Chromebook or components to other students *for any reason*. Students who do so are responsible for any loss of components.
16. Chromebooks come with a standardized image already loaded. These images may not be altered or changed in any way.
17. Students may not load or download any software, music, pictures, etc. on the Chromebook without specific instructions from a teacher to do so.
18. Educational Games may be used at the discretion of the teacher.
19. Chromebooks or other district issued electronic devices are to be carried in the school provided bags/carrying cases at all times.
20. All students have access to their Google drive on which to store data. It is the responsibility of the student to see to it that critical files are backed up regularly to this location.
21. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws.

General Reminders: Chromebooks At Home

1. District web filters are active at home, just as they are at school.
2. The use of Chromebooks at home is encouraged.
3. Chromebook care at home is as important as at school.
4. Transport your Chromebook in a case or protected backpack.
5. Listening to music on your Chromebook is allowed at home with permission from parents/guardians.
6. Online Gaming is allowed at home if all of the following conditions are met:
    a. content of game is school appropriate
    b. you have permission from your parent/guardian
    c. the game is in support of education
    d. all school work is complete
    e. no download of any kind is needed
7. Messaging is allowed at home if all the following conditions are met:
    a. the content of the messages are school appropriate
    b. the messages are in support of education
    c. you have permission from your parent/guardian

Terms of Use

Acceptable Use Policy

All users of the DCSD system and equipment must comply at all times with the ***Dansville Central School District Student Use of Computerized Information Resources - Policy 4526, Dansville CSD Technology USe Guide including Acceptable Use Policies.*** Any failure to comply may end your right of possession effective immediately. You may also be subject to disciplinary action.

Liability

If the property is not returned or is intentionally damaged, the student and family are responsible for the cost of repair or the replacement value on the date of the loss. In the case of theft, a police report must be filed within 48 hours and provided to the school, the building principal and the Technology Services Department. Failure to report the theft to the proper staff and follow the proper filing procedure will result in a full fine to the student. If the Chromebook is lost because of negligence, the student is responsible for the full replacement cost of the Chromebook.

Repossession

Failure to fully comply with all terms of this agreement may result in the confiscation of the Chromebook or other district issued electronic device the District at any time.
Unsupervised Chromebooks or other district issued electronic device will be confiscated by staff. Disciplinary action may be taken for leaving your Chromebook or other district issued electronic device in an unsupervised location.

Scheduled and Unscheduled Evaluations

Spot inspections of the Chromebooks or other district issued electronic device may occur regularly by technical support staff and/or administration. Some of the inspections will be scheduled through email and others will take place via remote connection to the Chromebook or other district issued electronic

device. Students with damaged Chromebooks or other district issued electronic device who fail to report the damage will be subject to fines and to discipline. Students with inappropriate content or programs will be subject to discipline and may also be fined.

Computer Rules and Regulations

Violations of these rules and guidelines will result in disciplinary action.

Acceptable Use Guidelines

The guidelines are provided here so that students and parents are aware of the responsibilities students accept when they use district-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, and Internet access. In general, this requires efficient, ethical and legal utilization of all technology resources.

Computer Use and Care

- Always carry your Chromebook in the DCSD Chromebook case.
- Use caution when carrying your Chromebook or other district issued electronic device in a crowded hallway. Carry it by the handles or shoulder strap and never swing the Chromebook or other district issued electronic device case around.
- No food or drink should be near Chromebooks or other district issued electronic devices
- When moving the Chromebook or other district issued electronic device, use two hands. Do not pick it up by the monitor.
- Close the Chromebook lid whenever you are not using it, or if you are moving it around.
- Never leave the Chromebook or other district issued electronic device unattended in the hallway or any other public space for any reason.
- When placing your Chromebook or other district issued electronic device in a locker, hang it in the carrying case on a coat hook. Never pile items on top of your Chromebook or other district issued electronic device.
- When placing your Chromebook or other district issued electronic device on a table or desk, gently position it on the surface. Do not slam/swing the Chromebook or other district issued electronic device onto the surface. Center the Chromebook or other district issued electronic device on desks or tables to avoid it being bumped and falling to the floor.
- Use your Chromebook or other district issued electronic device on a table. Do not use it on the floor or other unsteady surface.
- Keep your volume muted unless directed by a teacher.
- Lock your Chromebook or other district issued electronic device when it is not in use.
- When moving between classes, put your computer on Standby.
- When leaving for the day, completely shut down your Chromebook or other district issued electronic device.
- If at all possible, do not leave your Chromebook or other district issued electronic device in the car. If you must leave it, lock it in the trunk or somewhere out of view.
- Protect your Chromebook or other district issued electronic device from exposure to extreme heat or cold. This includes when leaving it in a vehicle.
- Students are prohibited from:
    - Putting stickers on the Chromebooks or other district issued electronic device, cases, batteries, or chargers.
    - Defacing DCSD issued equipment in any way. This includes but is not limited to marking, painting, drawing or marring any surface of the Chromebooks or other district issued electronic device or any stitching on the case. If such action occurs, the student will be

fined the cost of repair.

Network Etiquette

- Be polite; messages typed in capital letters on the computer are equivalent to shouting and are considered rude.
- Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
- Pretending to be someone else when sending/receiving messages is considered inappropriate.
- Transmitting obscene messages or pictures is prohibited.
- Revealing personal addresses or phone numbers of the user or others is prohibited.
- Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Music/Movies: At School

Listening to music on your Chromebook or other district issued electronic device is not allowed during school hours without permission from the teacher.

Games: At School

Online gaming is not allowed during school hours unless you have been given permission by a teacher. Any games must be in support of education.

Messaging: At School

Messaging is not allowed during school hours without permission from the teacher. Permission will be given only for messaging that is useful in completing a school assignment. All communication must be related to the school assignment.

Desktop Backgrounds and Screensavers

Students will have the ability to customize their desktop background by selecting one of the preloaded themes or images. They may also choose to use the standard background. Beyond that, students may not change the desktop background and screensaver.

Printing

Purpose of the chromebooks is to cut down on printing. Ultimately the district would like be to go paperless. All printing will be at the discretion of the teacher.

E-Mail

E-mail is to be used as a communication tool for school. One of the most common violations of the Acceptable Use guidelines by students is the sending of social or non-school related e-mail.

- E-mail should be used for educational purposes only.
- E-mail transmissions, stored data, transmitted data, or any other use of online services by students, employees or other users is not confidential and may be monitored by staff at any time to ensure appropriate use.
- All e-mail and all contents are property of the District.
- Classroom-based compliance checks may be conducted at any time. This means that teachers can check your e-mail.

Examples of Unacceptable Use

The following list covers the answers to some of the most frequently asked questions as well as the most common violations. This is not a comprehensive list.

Unacceptable conduct includes, but is not limited to the following:

1. Using the network for illegal activities, including copyright, license or contract violations, downloading inappropriate materials, viruses, and/or software, such as but not limited to

hacking and host file sharing software.

2. Using the network for financial or commercial gain, advertising, or political lobbying.
3. Accessing or exploring on-line locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as but not limited to pornographic sites.
4. Vandalizing and/or tampering with equipment, programs, files, software, system performance or other components of the network. Use or possession of hacking software is strictly prohibited.
5. Causing congestion on the network or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.
6. Gaining unauthorized access anywhere on the network.
7. Revealing the home address or phone number of one's self or another person.
8. Invading the privacy of other individuals.
9. Using another user's account, password, or allowing another user to access your account or password.
10. Coaching, helping, observing or joining any unauthorized activity on the network.
11. Forwarding/distributing E-mail messages without permission from the author.
12. Posting anonymous messages or unlawful information on the system.
13. Engaging in sexual harassment or using objectionable language in public or private messages, e.g., racist, terroristic, abusive, sexually explicit, threatening, stalking, demeaning or slanderous.
14. Falsifying permission, authorization or identification documents.
15. Obtain copies of, or modify files, data or passwords belonging to other users on the network.
16. Knowingly placing a computer virus on a computer or network.
17. Attempting to access or accessing sites blocked by the DCSD filtering system.
18. Downloading music, games, images, videos, or other media without the permission of a teacher.
19. Sending or forwarding social or non-school related e-mails.

Technology Discipline

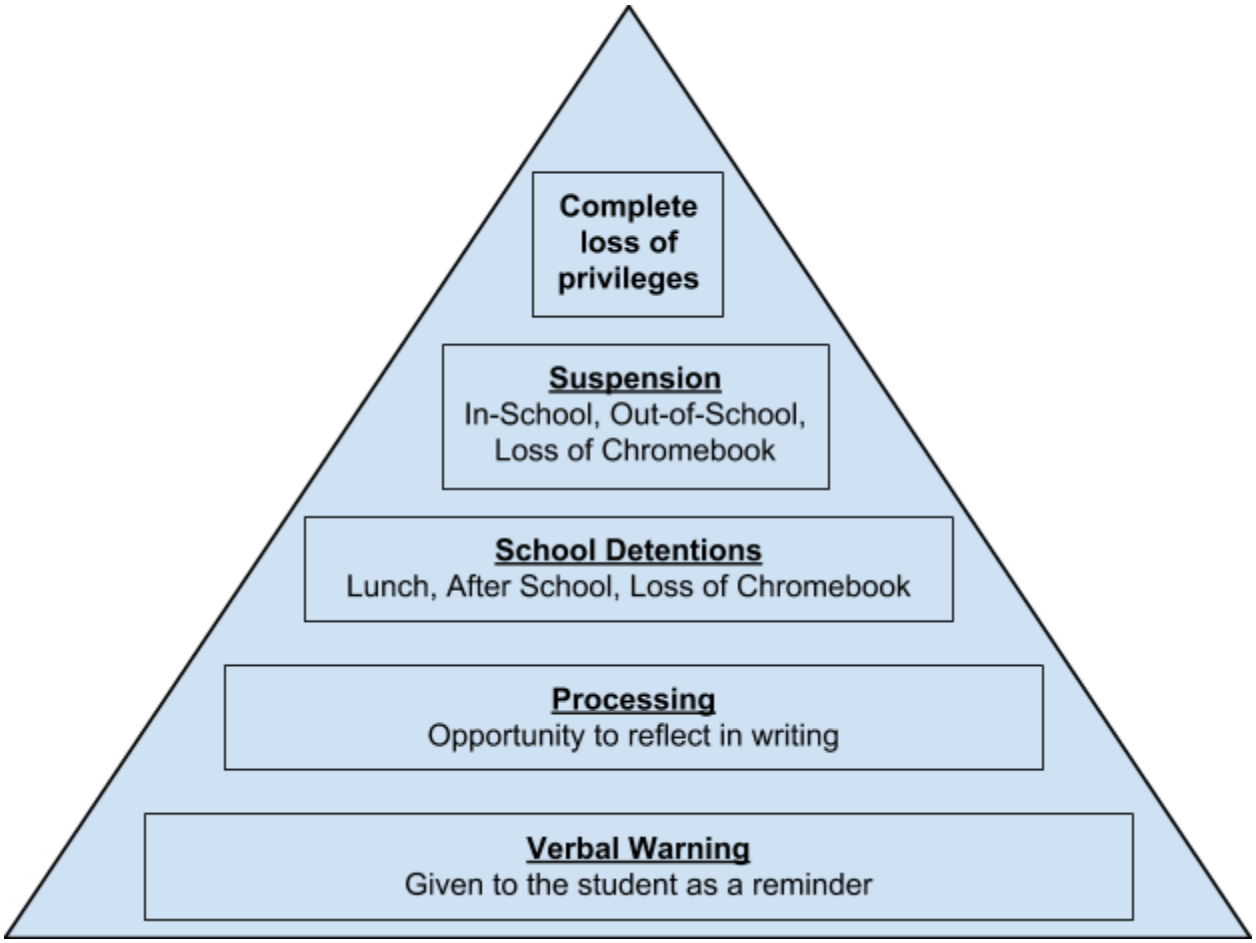
The discipline policies and Code of Conduct at each school have been revised to encompass the one-to-one environment. The privilege of having a computer comes with a new set of responsibilities and new consequences. The Technology Discipline Hierarchy has a common structure district-wide. These are explained in this section. Please reference the materials specific to each building and Code of Conduct for specific details or contact the school directly.

1. The Technology Discipline Hierarchy applies to all DCSD technology, not just Chromebook computers. This includes, but is not limited to iPads, SMARTBoards, Promethean Boards, document cameras, projectors, desktop computers, printers, mice, digital cameras, etc.
2. Discipline is progressive. Low-level, first-time infractions will have a lesser consequence than infractions that are repetitive or more serious in nature.
3. Classroom interventions will be the first level of discipline. This includes verbal warnings, seating changes, and teacher contact with home.
4. Discipline progresses in levels. Consequences include in-school detentions, after-school detentions, assignments that re-teach or reinforce correct behaviors, restricted computer access, office referrals, and suspensions.
5. Compliance checks may be conducted on a student's computer at any time. These may be school-wide checks or conducted individually due to suspicion of inappropriate computer usage.

6. DCSD may remove a user's access to the network without notice at any time if the user is engaged in any unauthorized activity.

Example:

Technology Discipline Hierarchy



Computer Security

Each of the Chromebooks and other district issued electronic device are managed by DCSD. We have tried to strike a balance between usability of the equipment, and appropriate security to prevent the units from being damaged or used to cause damage to the Dansville Central School District system. Two primary forms of security exist:

Desktop Security

Security is in place on the desktop to prevent and/or track certain activities. These include downloading or installing software on the Chromebooks or other district issued electronic device, removing software, changing system settings, etc.

Filtering/Monitoring Software

DCSD maintains an Internet filtering/monitoring solution. This program automatically filters all student access to the Internet and monitors student activities on the computer both in school and at home. Please note, however, that there is no better security tool than an involved adult!

Damaged Equipment

Repairs

Occasionally, unexpected problems do occur with the Chromebooks or other district issued electronic device that are not the fault of the user (computer crashes, software errors, etc.). The Technology Services Department is prepared to assist students in resolving these issues. These issues will be remedied at no cost.

Loaner Chromebooks – "Hot Spares"

Temporary replacements, known as a Hot Spares, are also available in the Technology Services Department so that student learning is not disrupted by the repair process. Students are responsible for the care of the swap while it is issued to them. All of the same rules and regulations apply to swap computers, and students are expected to treat them as if they were their own. Students are required to save to their Google Drive in case they need to be issued a Swap.

Accidental Damage vs. Negligence

Accidents do happen. There is a difference, however, between an accident and negligence. The price that the district paid for the Chromebook includes: the Chromebook or other district issued electronic device, case, and a one year warranty. The Chromebook or other district issued electronic device warranty will cover normal wear and tear along with other damage that might occur during normal use of the Chromebook or other district issued electronic device. After investigation by school administration, if the Chromebook or other district issued electronic device is deemed to be intentionally or negligently damaged by the student, the student may be subject to discipline and the cost of repair or replacement and a swap will not be provided.

Lost or Stolen Equipment

In this section, "equipment" refers to Chromebooks or other district issued electronic device, chargers and cases. Chromebooks or other district issued electronic device and other equipment are issued as an educational resource. The conditions surrounding this equipment can be equated to those of a textbook or a school issued calculator. Students are expected to keep track of and to care for this equipment for the time period it is issued to them. Students/families may be fined for damaged or lost equipment.

Lost Equipment

Reporting Process

If any equipment is lost, the student or parent must report it to the school immediately. Students can let a teacher or administrator know, and the staff member will assist him/her.

Financial Responsibility

The circumstances of each situation involving lost equipment will be investigated individually.

Stolen Equipment

Student Safety

It is always a high priority to ensure the safety of our students while at school and we hope these precautions will help students be safe on the path to and from school. Student safety always comes first. If a student is faced with an unsafe situation, such as theft, the student is advised to let the assailant have the equipment and to immediately contact the police.
Please review the following safety tips:

- Leave home on time so that you get to school on time.

- Walk to and from school in groups of two or more.
- Always be aware of your surroundings including people and vehicles.
- Let someone know when you leave and when you arrive back home.
- Always follow the safest route to school. Use main streets; avoid dimly lit areas, alleys, backyards, shortcuts and abandoned buildings.
- If someone follows you on foot, get away from him or her as quickly as possible.
- If someone follows you in a car, turn around and go in the other direction.
- Always tell a parent, guardian, school official, or another trusted adult what happened.
- Obey the traffic lights.
- Cross the street when the signal says walk or when there is a green light.
- Look both ways and never run across the street.
- Turn the pockets of the Chromebook or other district issued electronic device case in toward your body to not look as obvious.
- If someone demands your Chromebook or other district issued electronic device, give it to them.

Reporting Process

If any equipment is reported as stolen, a police report must be filed within 48 hours and a copy of the report must be provided to the building principal or the Director of Technology by the student or parent. If there is not clear evidence of theft, or the equipment has been lost due to student negligence, the student and parent will be responsible for the full cost of replacing the item(s).

Financial Responsibility

The circumstances of each situation involving stolen equipment will be investigated individually.

Fees, Fines, and Repair Costs

- Students are expected to keep the Chromebooks or other district issued electronic device in good condition. Failure to do so will result in fines as specified below.
- Students are expected to report any damage to their computer as soon as possible. This means no later than the next school day.
- Spot checks of Chromebooks or other district issued electronic device may occur regularly.
- Students who fail to report damage or abuse will be subject to fines and to discipline.
- Inappropriate media may not be used as a desktop background. In addition, changing wallpaper means downloading pictures, which is prohibited and will result in disciplinary action.
- Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, and/or gang related symbols will result in disciplinary action, or loss of Chromebook or other district issued electronic device privileges.

Damage and Fine List - for reckless or intentional damage or loss

Estimated Item Replacement Cost

Chromebook Case $20.00
Power Cord $40.00
Chromebook $250.00
Full Package $270.00

Estimated Damage Fines

Cracked Screen $75.00
Broken Latch $25.00
Broken Chassis $25.00

Broken Keyboard $25.00
Broken or Missing Keys $15.00-$25.00
Damaged Power Cord $40.00
Lost/Damaged Case $20.00
Unreported Lost/Stolen Chromebook $270.00
Intentional Cosmetic Damage $15.00-full cost of item

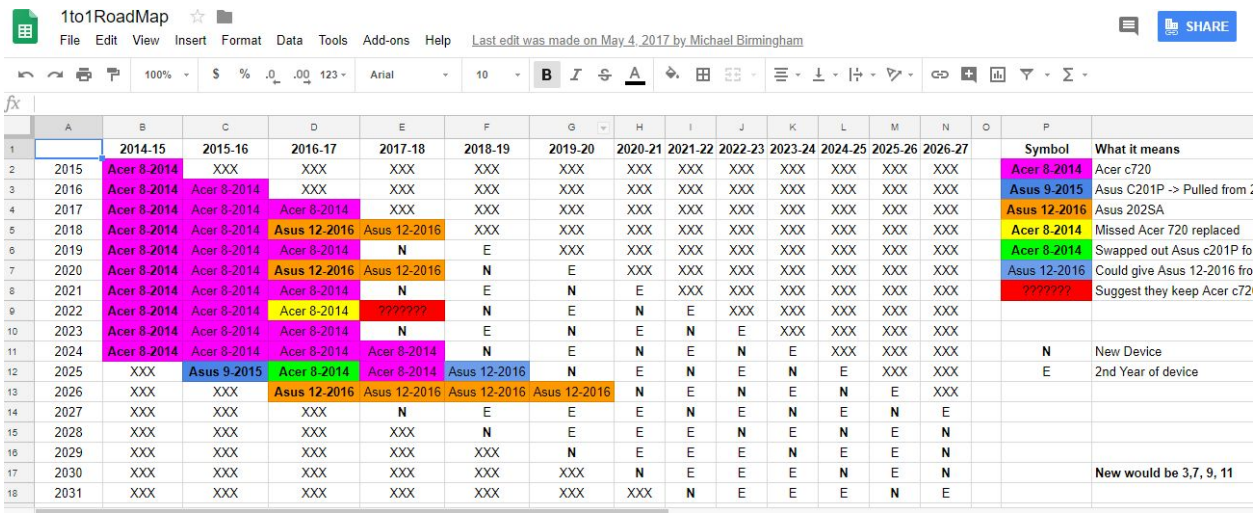
APPENDIX E:

DCS 1:1 RoadMap

The Dansville Central School District maintains a 1:1 Roadmap which serves as our replacement schedule to ensure that student and staff Chromebooks are regularly replaced.

In a similar fashion we regularly replace desktops provided for faculty in all buildings. We are developing a replacement schedule for iPads which are provided for Primary School Faculty and students.

Example of the roadmap:



1to1RoadMap

File Edit View Insert Format Data Tools Add-ons Help Last edit was made on May 4, 2017 by Michael Birmingham

SHARE

	2014-15	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27
2015	Acer 8-2014	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2016	Acer 8-2014	Acer 8-2014	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2017	Acer 8-2014	Acer 8-2014	Acer 8-2014	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2018	Acer 8-2014	Acer 8-2014	Asus 12-2016	Asus 12-2016	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2019	Acer 8-2014	Acer 8-2014	Acer 8-2014	N	E	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2020	Acer 8-2014	Acer 8-2014	Asus 12-2016	Asus 12-2016	N	E	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2021	Acer 8-2014	Acer 8-2014	Acer 8-2014	N	E	N	E	XXX	XXX	XXX	XXX	XXX	XXX
2022	Acer 8-2014	Acer 8-2014	Acer 8-2014	???????	N	E	N	E	XXX	XXX	XXX	XXX	XXX
2023	Acer 8-2014	Acer 8-2014	Acer 8-2014	N	E	N	E	N	E	XXX	XXX	XXX	XXX
2024	Acer 8-2014	Acer 8-2014	Acer 8-2014	Acer 8-2014	N	E	N	E	N	E	XXX	XXX	XXX
2025	XXX	Asus 9-2015	Acer 8-2014	Acer 8-2014	Asus 12-2016	N	E	N	E	N	E	XXX	XXX
2026	XXX	XXX	Asus 12-2016	Asus 12-2016	Asus 12-2016	Asus 12-2016	N	E	N	E	N	E	XXX
2027	XXX	XXX	XXX	N	E	E	E	N	E	N	E	N	E
2028	XXX	XXX	XXX	XXX	N	E	E	E	N	E	N	E	N
2029	XXX	XXX	XXX	XXX	XXX	N	E	E	E	N	E	E	N
2030	XXX	XXX	XXX	XXX	XXX	XXX	N	E	E	E	N	E	N
2031	XXX	XXX	XXX	XXX	XXX	XXX	XXX	N	E	E	E	N	E

Symbol	What it means
Acer 8-2014	Acer c720
Asus 9-2015	Asus C201P -> Pulled from
Asus 12-2016	Asus 202SA
Acer 8-2014	Missed Acer 720 replaced
Acer 8-2014	Swapped out Asus c201P fo
Asus 12-2016	Could give Asus 12-2016 fro
???????	Suggest they keep Acer c72
N	New Device
E	2nd Year of device
New would be 3,7, 9, 11	

APPENDIX F:

Dansville School District
Acceptable Use Policy (AUP)

This policy may be amended at any time.
Legal Authorization: Education Law Sections 1604, 1709, 1804

Purpose
The Dansville Board of Education provides a computer system including the Internet to:

- promote educational excellence
- promote resource sharing
- promote innovative instruction
- promote communication
- prepare students to live and work in the 21st century

Teachers, other members of the instructional staff, and administrators are authorized to use the computer system and connections for instruction, professional development, training, research and communications related to curriculum. Students are also authorized to use the computer system for educational research and communication. The computer system includes all hardware, software, data communication lines and devices, terminals, printers, CD-ROM devices, tape driver, servers, server and personal computers, the Internet, email, local and wide area networks, and the use of wireless network with personal devices (BYOD/Bring Your Own Device).

Use of the system during school and professional hours must be (1) in support of education and or research, (2) for school business, (3) in support of the mission of Dansville Central School, and (4) in accordance with all Board of Education policies and state and federal regulations.

The computer system will also assist in sharing information with the local community including parents, local, state and federal government agencies, and businesses.

Access to the Dansville Central School computer system is a privilege and not a right. Violation of any of the provisions described below will result in disciplinary action.

District Responsibility
The technology staff shall provide the following services including but not limited to:

- Establishing individual and class accounts (server based and online)
- Setting quotas for disk usage on the system
- Devising a district virus protection procedure

Dansville Central School district will provide the following services including, but not limited to:

- Email accounts for staff and students in certain curriculum
- Internet access
- A filtering system

Acceptable Use
Effective performance of computer and telecommunication networks, whether local or global, relies upon end users adhering to established standards of proper conduct. In general, this requires efficient, ethical, and legal utilization of network resources. Use of the Dansville School computer system must be consistent with the educational objectives and mission of the district.

Any employee or student who fails to comply with the terms of this policy or the regulations developed by the Superintendent may lose system privileges. Employees may also be disciplined by the Superintendent up to and including termination depending upon the nature of the violation of this policy or the implementing regulations Students may be disciplined in accordance with the district Code of Student Conduct. Employees and students may also be subject to appropriate legal action for violation of this policy or implementing regulations.

Each employee, student, and parent or guardian is advised of this Acceptable Use Policy and the DCSD Master Technology Plan. In addition it is posted on the DCSD Website, and upon login on district computers

This is not intended to be an exhaustive list. Students, parents or staff who have questions about prohibited activities are encouraged to contact a building administrator.

A Illegal Activities

- Attempts to gain unauthorized access to accounts
- Use of an account not assigned to the individual
- Vandalism is not permitted and will be strictly disciplined
- Transmission of any material in violation of any law is prohibited. This includes but is not limited to: copyrighted materials, threatening or obscene materials, or material protected by trade secrets.
- Users will not plagiarize any materials from the Internet
- Users will not attempt to circumvent or bypass filtering system
- Users will not install or attempt to install any updates or upgrades to computer software
- Users will not install software on computers

B. System Security

- Network accounts shall be used by authorized owners only
- Passwords should be kept private and changed frequently
- Users will immediately notify the instructor in charge if they have identified a possible security problem

C. Inappropriate Language

- Students and employees will conduct themselves in a manner that is appropriate and properly represents Dansville School District while online
- Use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language is expressly forbidden
- Information will not be posted that, if acted upon, could cause damage or a danger of disruption
- Users will not harass or otherwise engage in personal attacks
- Users will not participate in any form of cyber bullying

D. Inappropriate Use of System

- Use of IRCs (Internet Relay Chats, or similar services) is prohibited
- Internet use for commercial purposes, financial gain, personal business, product advertisements, or political lobbying is prohibited
- Users will not download large files unless absolutely necessary
- Users will not use excessive data storage or network bandwidth
- Users will not engage in spamming
- Educational games will be permitted at the discretion of the instructor providing that the student is passing and all school work is complete.
- Users shall not use proxy sites, services, or programs to bypass internet filtering

E. Personal Safety (Restrictions are for students only)

- Personal information such as addresses, phone numbers, financial information, or non-district e-mail addresses shall not be included in network communications
- Students will not agree to meet with someone they have met online through the school computer system
- Students will promptly notify the instructor in charge if they receive any message that is inappropriate, offensive or makes them feel uncomfortable

- Personal email usage during school hours is expressly prohibited
- Students using personal devices are still subject to all school rules and regulations

Limitation of Liability
The Dansville School District makes no warranties of any kind, whether express or implied, for the service it is providing. The District will not be responsible for any damages suffered while on the system. These damages may include loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by negligence, errors or omissions. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services. Further, the district is not responsible for any unauthorized charge or fee resulting from use of the school computer system.

Right of Privacy
Employees and students have no right of privacy and should have no expectation of privacy in materials sent, received, or stored in the Dansville School computer system.

Parental Notification and Responsibility
The Dansville Central School District will notify parents and legal guardians about the computer systems and the Board of Education Policy and Regulations governing its use. A parent who does not want their child(ren) to have access to the Internet and/or email should contact the school principal. Parents and legal guardians have the right to revoke their permission and terminate the student's Internet access at any time. *The school will provide information to the parents about the filtering software.*

There is a wide range of material available on the Internet, some of which may not fit the values of particular families. It is not possible for the school district to monitor and enforce social values in student use of the Internet. Further, the school district recognizes that parents bear the primary responsibility for transmitting their particular set of family values to their children; therefore, the school encourages parents to specify to their child(ren) what material is and is not acceptable.

Violations/Due Process
The Dansville Central School District will cooperate fully with local, state and federal officials in any investigation concerning or relating to any illegal activities conducted through the computer system. In the event that there is an allegation that a student or employee has violated the district's Acceptable Use Policy or the provisions of this regulation, the student or employee will be presented with the charges and provided an opportunity to present an explanation before further disciplinary actions are taken.

Disciplinary actions will be tailored to meet the specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to behave appropriately on an electronic network. Disciplinary actions are in accordance with the Dansville Code of Conduct and may include the following:
- Removal from the network
- Suspension
- Law enforcement involvement

Search and Seizure
An individual search may be conducted when there is reasonable suspicion that the user has violated the law, the Code of Student Conduct, or School Board Policy. The nature of the search/investigation will be reasonable and in keeping with the nature of the alleged misconduct as per the Acceptable Use Policy.

System users have no right of privacy and should have no expectation of privacy in materials sent, received or stored in school owned computers or on the district computer system.

Glossary

Term	Description
Harassment	Persistently acting in a manner that distresses or annoys another person.
Plagiarize	To take the ideas or writing or others and presenting them as if they were original to the user.
Spamming	Sending an annoying or unnecessary message to a large number of people.
Vandalism	Any attempt to harm or destroy data of another user, agency or network including uploading, downloading, or creating computer viruses.

What is Blocking/Filtering Software:

Blocking/Filtering software is a mechanism used to:

- restrict access to Internet content, based on an internal database of the product, or:
- restrict access to Internet content through a database maintained external to the product itself, or:
- restrict access to Internet content to certain ratings assigned to those sites by a third party or;
- restrict access to Internet content by scanning text, based on a keyword or phrase or text string, or;
- restrict access to Internet content by scanning pixels, based on color or tone, or;
- restrict access to Internet content based on the source of the information

Full Dansville Master Technology Plan on the District Website: Click on Departments, Computer Technology

APPENDIX G:

FERPA:
Dansville School District Annual FERPA Notification & Opt out form

The Dansville School District follows the guidelines of the Family Educational Rights and Privacy Act (FERPA) regarding all student records. The district proposes to designate the following personally identifiable information contained in a student's education records as "directory information."

1. Student's name
2. Student's address
3. Telephone number(s)
4. Student's date and place of birth
5. Participation in officially recognized activities and sports
6. Student's achievement awards or honors
7. Student's weight and height, if a member of an athletic team
8. Major field of study
9. Dates of attendance ("from and to" dates of enrollment)
10. Date of graduation
11. Student's photos

The above information is disclosed without prior written consent, except when the request is for a profit-making plan or activity. Student records that consist of "personally identifiable information" generally are exempt from disclosure. Student directory information, however, is released unless the parents have affirmatively withdrawn their consent to release in writing.

Administrative regulations set forth a procedure for annual notification to parents and eligible students of the District's definition of directory information. Parents or eligible students then have two weeks in which to advise the District, in accordance with such regulations, of any or all items which they refuse to permit as directory information about that student.

If the release of this information is deemed acceptable, you need do nothing with this sheet. If you do not wish this information or any part of it to be provided to requesting parties, please sign and date below, print the name of your student along with the directory information you do not want released, and return this form to your school office.

Please understand that if you advise us that all or any part of this directory information about your student is not to be released, then we are prohibited by law from releasing that information to anyone, including representatives of the armed forces, businesses, industries, charitable institutions, other employees, and institutions of higher education.

_____ _____

Student's Name and Grade (Please Print) Signature

_____

APPENDIX H: Parent Bill of Rights

Dansville CSD Parent Bill of Rights

PARENTS' BILL OF RIGHTS
FOR DATA PRIVACY AND SECURITY

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, "educational agencies" (as defined below) in the State of New York collect and maintain certain personally identifiable information from the education records of their students. As part of the Common Core Implementation Reform Act, Education Law §2-d requires that each educational agency in the State of New York must develop a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights). The Parents' Bill of Rights must be published on the website of each educational agency, and must be included with every contract the educational agency enters into with a "third party contractor" (as defined below) where the third party contractor receives student data, or certain protected teacher/principal data related to Annual Professional Performance Reviews that is designated as confidential pursuant to Education Law §3012-c ("APPR data").

The purpose of the Parents' Bill of Rights is to inform parents (which also include legal guardians or persons in parental relation to a student, but generally not the parents of a student who is age eighteen or over) of the legal requirements regarding privacy, security and use of student data. In addition to the federal Family Educational Rights and Privacy Act (FERPA), Education Law §2-d provides important new protections for student data, and new remedies for breaches of the responsibility to maintain the security and confidentiality of such data.

A. What are the essential parents' rights under the Family Educational Rights and Privacy Act (FERPA) relating to personally identifiable information in their child's student records?

The rights of parents under FERPA are summarized in the Model Notification of Rights prepared by the United States Department of Education for use by schools in providing annual notification of rights to parents. It can be accessed at
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html

Complete student records are maintained by schools and school districts, and not at the New York State Education Department (NYSED). Further, NYSED would need to establish and implement a means to verify a parent's identity and right of access to records before processing a request for records to the school or school district. Therefore, requests to access student records will be most efficiently managed at the school or school district level.

Parents' rights under FERPA include:

1. The right to inspect and review the student's education records within 45 days after the day the school or school district receives a request for access.

2. The right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Complete student records are maintained by schools and school districts and not at NYSED, which is the secondary repository of data, and NYSED make amendments to school or school district records. Schools and school districts are in the best position to make corrections to students' education Records.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to:

- (i) school officials within the school or school district with legitimate educational interests;
- (ii) officials of another school for purposes of enrollment or transfer;
- (iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED;
- (iv) (v) organizations conducting studies for or on behalf of educational agencies) and
- (vi) the public where the school or school district has designated certain student data as "directory information" (described below). The attached FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).

4. Where a school or school district has a policy of releasing "directory information" from student records, the parent has a right to refuse to let the school or school district designate any all of such information as directory information. Directory information, as defined in federal regulations, includes: the student's name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent's refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.

5. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA. B. What are parents' rights under the Personal Privacy Protection Law (PPPL), Article 6-A of the Public Officers Law relating to records held by State agencies?

The PPPL (Public Officers Law §§91-99) applies to all records of State agencies and is not specific to student records or to parents. It does not apply to school districts or other local educational agencies. It imposes duties on State agencies to have procedures in place to protect from disclosure of "personal information," defined as information which because of a name, number, symbol, mark or other identifier, can be used to identify a "data subject" (in this case the student or the student's parent). Like FERPA, the PPPL confers a right on the data subject (student or the student's parent) to access to State agency records relating to them and requires State agencies to have procedures for correction or amendment of records.

A more detailed description of the PPPL is available from the Committee on Open Government of the New York Department of State. Guidance on what you should know about the PPPL can be accessed at http://www.dos.ny.gov/coog/shldno1.html

The Committee on Open Government's address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1. What "educational agencies" are included in the requirements of Education Law §2-d?

- The New York State Education Department ("NYSED");
- Each public school district;
- Each Board of Cooperative Educational Services or BOCES; and
- All schools that are:
    - a public elementary or secondary school;
    - a universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
    - an approved provider of preschool special education services;
    - any other publicly funded pre-kindergarten program;
    - a school serving children in a special act school district as defined in Education Law 4001; or
    - certain schools for the education of students with disabilities - an approved private school, a state-supported school subject to the provisions of Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

2. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term "student" refers to any person attending or seeking to enroll in an educational agency, and the term "personally identifiable

information" ("PII") uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII includes, but is not limited to:

- (a) The student's name;
- (b) The name of the student's parent or other family members;(c) The address of the student or student's family;
- (d) A personal identifier, such as the student's social security number, student number, or biometric record;
- (e) Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name

Please note that NYSED does not collect certain information defined in FERPA, such as students' social security numbers, biometric records, mother's maiden name (unless used as the mother's legal name).

- (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

3. What kind of student data is not subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de- identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents' Bill of Rights.

4. What are my rights under Education Law § 2-d as a parent regarding my student's PII?

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

- (A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.
    - o PII may be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.

    - o However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.
- (B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.
    - This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
    - o NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.
    - o The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.
- (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.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

- (A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;
- (B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and
- (C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.
- (D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and
- (E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department,

89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. The complaint process is under development and will be established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.

- o Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third party contractor or its officers, employees or assignees.
- o When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

5. Must additional elements be included in the Parents' Bill of Rights.?

Yes. For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

- (A)the exclusive purposes for which the student data, or teacher or principal data, will be used;
- (B) how the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- (C) when the agreement with the third party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- (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; and
- (E) where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
    - a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in Regulations of the Commissioner.

6. What protections are required to be in place if an educational agency contracts with a third party contractor to provide services, and the contract requires the disclosure of PII to the third party contractor?

Education Law §2-d provides very specific protections for contracts with "third party contractors", defined as 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 such educational agency. The term “third party contractor” also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an “educational agency.”

Services of a third party contractor covered under Education Law §2-d include, 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. When an educational agency enters into a contract with a third party contractor, under which the third party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy.

However, the standards for an educational agency’s policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents’ Bill of Rights must be included, as well as a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Each third party contractor that enters into a contract or other written agreement with an educational agency under which the third party contractor will receive student data or teacher or principal data shall:

- o limit internal access to education records to those individuals that are determined to have legitimate educational interests
- o not use the education records for any other purposes than those explicitly authorized in its contract;
- o except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party
    - (i) without the prior written consent of the parent or eligible student; or
    - (ii) unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
        - o maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
        - use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

7. What steps can and must be taken in the event of a breach of confidentiality or security?

Upon receipt of a complaint or other information indicating that a third party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third party contractor's facilities and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data or teacher or principal APPR data. Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay;

- (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

8. Data Security and Privacy Standards

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

9. No Private Right of Action
Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.

ATTACHMENT

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of school ("School")] receives a request for access. Parents or eligible students should submit to the school principal [or appropriate school official] a written request that identifies the records they wish to inspect. The school official will make arrangements for access

and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. Parents or eligible students who wish to ask the [School] to amend a record should write the school principal [or appropriate school official], clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

[Optional] Upon request, the school discloses education records without consent to officials of another school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW

Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by §99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that elementary and secondary schools may make without consent. FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student – To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))

To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))

To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency in the parent or eligible student's State (SEA).

Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35) In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4)) To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))
To organizations conducting studies for, or on behalf of, the school, in order to:

- (a) develop, validate, or administer predictive tests;
- (b) administer student aid programs; or
- (c) improve instruction. (§99.31(a)(6))

To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7)) To parents of an eligible student if the student is a dependent for IRS tax purposes.(§99.31(a)(8))
To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))
To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)
Information the school has designated as “directory information” under §99.37. (§99.31(a)(11))

APPENDIX I: Code of Conduct Documents

DCS Code of Conduct

APPENDIX J: Technology Committee and Collaborators

Member	Title	Email
Dr. Paul Alioto	DCS Superintendent	aliotop@dansvillecsd.org
Lynne Blum	HS Library/Media Specialist	bluml@dansvillecsd.org
Joie Petrillo	DCS PS	petrilloj@dansvillecsd.org
Jim Blum	DCS Tech. Coordinator	blumj@dansvillecsd.org
Kim Derrenbacher	Tech PD and District PR	measek@dansvillecsd.org
Mike Birmingham	DCS Network Administrator	birminghamm@dansvillecsd.org
Barbara Pamper	Curric/Technology Admin	pamperb@dansvillecsd.org
Kevin Geiger	MST LAB Teacher	geigerk@dansvillecsd.org
Velma Kahn	Computer Teaching Asst.	kahnv@dansvillecsd.org
Janelle Rinker	Primary Library Media Specialist	rinkerj@dansvillecsd.org
Emily Wolf	EBH Library Media Specialist	wolfe@dansvillecsd.org
Lisa Johnson	EBH Principal	johnsonl@dansvillecsd.org
Jen Migliore	HS 9/10 Special Education	migliorej@dansvillecsd.org
Ani Rosario	HS ELA	rosarioa@dansvillecsd.org
Teegan Pearson	HS Special Education	pearsont@dansvillecsd.org