

# DANSVILLE CENTRAL SCHOOL



*Leaders in Technology for Learning*

## **2022-2025 Technology Plan**

Updated September 22, 2015

June 2016

June 2017

June 2018

June 2022

# TABLE OF CONTENTS

[Dansville Vision & Mission Statements](#)

[Technology Mission Statement](#)

[District Action Plan 2022 - 2025](#)

[DCS Computer Technology Infrastructure](#)

[Internet Safety Plan](#)

[Addendum](#)

# 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 Vision Statement

The mission of Dansville Central School District Technology Plan is to support sustaining and improving collaborative learning environments for all, in which our students can achieve their full potential especially in reaching NYS Next Gen Learning Standards and contribute to our evolving local and global communities. The goal is for students to transition from consumers of information to creative producers and owners of knowledge. Specifically we aspire for our students to be:

- ★ Immersed in instruction aligned to NYS Next Gen Learning Standards that actively engages them, sparks creativity and transforms their learning
- ★ Critical thinkers who seek 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
- ★ Able to equitably access technology and learning at all times

## Master Technology Plan 2022-25 Introduction

Instructional Technology has been a focus of extreme importance to the Dansville Central School District for over 10 years and particularly since becoming a 1:1 district in the 2014-15 school year. During the pandemic the district became even more acutely aware of the critical role of technology in supporting student learning and effective teaching. Equally important was and is ensuring equitable access to technology for all students and staff. The district sprang to action with developing and

providing professional learning and assisting students and families with access to technology. With this 2022-25 comprehensive plan we seek to continue and expand both professional learning and equitable access, as well as maintaining our place as Leaders in Technology for Learning.

To ensure DCSD students exemplify the drive capability and compassion to achieve their full potential, we are committed to leveraging the best of what we learned in remote and hybrid teaching, to transform student learning from passive to creative. In addition, as we enter full implementation of NYS Next Gen Learning standards, we plan to leverage our learning to close gaps and assure our students achieve the learning set by these standards. We plan to achieve this through collaborative colleague-to-colleague professional learning that seeks to integrate effective instructional technology and curriculum.

Learning in the digital age becomes problematic if not impossible without a strong emphasis on digital citizenship and a robust cybersecurity environment. Digital citizenship refers to **responsible technology usage**, and teaching digital citizenship is essential to helping students achieve and understand digital literacy, as well as ensuring cyberbullying prevention, online safety, digital responsibility, and digital health and wellness. DCSD remains committed to the PK-12 digital citizenship curriculum.

Cybersecurity refers to the network, equipment and data and the protection of all 3. Cybersecurity is a key focus of DCSD both the protection of student data as well as the integrity and protection of the digital environment. DCSD has implemented the provisions of EdLaw2-d and is using the NIST Cybersecurity Framework to improve infrastructure in 5 key areas. This work is a major goal of the 2022-25 comprehensive technology plan.

Effective instructional technology including equitable access, digital citizenship and robust cyberserity environment form the basis of the DCSD's 2022-25 comprehensive technology plan. The Board of Education, district staff and community members all play a key role in commitment to ensuring its successful implementation.

#### District Goals 2022-2025

1. Increase equitable access to high-quality digital resources and standards-based, technology-rich learning experiences both in school and away from school.
2. Sustain and Expand safe, responsible, and educational technology use through continued and enhanced Digital Citizenship, Technology Skills, and STEAM curriculum PK-12.
3. Enhance the Cybersecurity infrastructure to provide the safety and security of all while simultaneously bringing the world of learning to our students.
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 equitable access to a digitally rich curriculum, instruction, and assessment program 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:

- Ensure equitable access to all our students
- Maintain a safe technology environment that ensures the privacy and security of our students and staff
- Solve complex problems
- Work collaboratively, locally, nationally and globally
- Communicate effectively
- Prepare students for college acceptance or for alternative paths to workplace readiness
- Achieve NYS Next Gen Learning and Content Standards aligned instruction
- Student self-directed learning
- Assess instructional efficacy both formative and summative
- Improve student academic achievement through increased participation and engagement
- Accommodate different curriculum needs and different learning styles

## **District Commitments:**

The District Administration and IT Staff are committed to:

1. Ensuring equitable access to information and technologies needed to function as productive members of the 21st century society
2. Supporting teachers in creating and sustaining instructional technology that puts students in creative and interactive relationship with technology that amplifies and transforms learning and achievement
3. Providing and encouraging ongoing Professional Learning in and out of the classroom
4. Offering and encouraging participation in district-wide opportunities for continual technological education for students, parents, and community.
5. Ensuring the continuity and coordination of acquisition, application, replacement, and maintenance of changing technology.
6. Moving beyond 1:1 to ensuring each and every classroom is equipped with a standard set of high quality instructional technology
7. Encouraging, Planning, and supporting district and building efforts to promote and enforce responsible technology through Digital Citizenship programs and instruction

# District Action Plan 2022-2025

**Goal 1: Increase equitable access to high-quality digital resources and standards-based, technology-rich learning experiences both in school and away from school Teachers / Staff**

**Action Plans:**

- A. Provide and support professional learning in technology-enhanced, culturally-and linguistically-responsive learning environments to support improved teaching and learning. DCSD has embarked on programs to enhance a culturally-and linguistically-responsive learning environment:
  - i. DEI - delving into diversity, equity and inclusion to implement action plans collaboratively developed to promote culturally responsive classrooms and school environments that support improved and inclusive learning as well as family and community engagement.
  - ii. Tier 1 Commitment to Active Student engagement in learning through unleashing the Science of Learning. Book Study of *Powerful Teaching* and reengagement with Kagan Cooperative Learning.
  - iii. Restorative Practices - ensuring our behavior management practices are restorative and healing rather than simply punitive.
  - iv. Strategic Planning: Needs Assessment - DCSD is engaging in a comprehensive needs assessment with a woman-owned consulting business to create a 5 year Strategic Plan.
- b. Collaborate and Plan for Equitable Technology Support - Ensure equitable access to digitally rich curriculum, assessment, and instruction. This includes assistive technology for students with disabilities and English language learners.
- c. Provide and maintain PK-12 Technology Integration into curriculum including digital citizenship, coding, and technology skills as well as STEAM
- B. Design and deploy high quality technology devices in support of 21st Century Learning in each and every classroom PK-12
  - a. Develop multi-year plan to ensure each classroom has high quality, reliable technology infrastructure to support cutting edge teaching and learning
    - i. Desktop
    - ii. Interactive Whiteboard
    - iii. High Speed Internet Connectivity
- C. Ensure all students have adequate access to technology away from home going beyond 1:1 to marshaling resources to assist with accessibility for all students.
  - a. Collaborate with EduTech, NYSED and federal government on ensuring all

families have access to high quality Internet connectivity

- i. Hot spots
- ii. Connection to federal / state assistance with costs of internet
- iii. Collaborate with federal / state government in bringing internet access to all parts of our community

D. Provide access to relevant and rigorous professional learning to ensure educators and leaders are proficient in the integration of learning technologies. DCSD has been 1:1 since 2014-15 and is always seeking ways to innovate. This 3 year period will be focused primarily on creating culturally responsive teaching and learning that seeks to engage students in learning by connecting to who they are and harnessing student cultural background in increasing student learning. Technology provides excellent opportunities to provide students with windows and mirrors - mirrors reflecting their own experiences and background and windows bringing the experiences of others to their learning.

- E. Create and sustain opportunities for colleague to colleague professional learning in effective pedagogy employing instructional technology in transformative ways.
- a. Engage staff in study of *Powerful Teaching*.
    - i. Provide re-introduction to Kagan Cooperative Learning
    - ii. Promote Instructional Technology that seeks to put students in creative and interactive environments that amplifies and transforms learning and student achievement.
    - iii. Professional Learning after school, SCDs, dept/grade level meetings

**F. BUDGET:**

- a. Professional Learning (Part of Curriculum and Instruction) - \$236,000 - annual
- b. Desktop and Interactive Whiteboard replacement (multi-year plan) - \$520,000 over 5- 7 years
  - i. SMART bond funds
  - ii. Federal funds
  - iii. BOCES - EduTech
  - iv. District Technology Budget
- c. ECF Funds possible for Hotspots
- d. eRate for access point and wireless enhancement

**G. TIMELINE:**

- a. Professional learning ongoing annually
- b. Desktop and Whiteboard replacement plan - 2022-29
- c. ECF Hotspots - 2020 - 2022
- d. eRate - 2022-23

**Goal 2: Sustain and Expand safe, responsible, and educational technology use through continued and enhanced Digital Citizenship, Technology Skills, and STEAM curriculum PK-12.**

- I. **Digital Citizenship - ISTE Defines Digital Citizenship as:** “the ability for students to “recognize the rights, responsibilities, and opportunities of living, learning and working in an interconnected digital world.” Digital citizenship refers to **responsible technology usage**, and teaching digital citizenship is essential to helping students achieve and understand digital literacy, as well as ensuring cyberbullying prevention, online safety, digital responsibility, and digital health and wellness. The DCS Digital Citizenship Curriculum is based on Common Sense Media. From Common Sense Media: “Learning never stops, and neither does digital citizenship. Teaching our students digital skills and inviting them to reflect on how media and technology affect their daily lives is essential to helping them connect with the world around them” As we emerge from the pandemic to a “new normal” Digital Citizenship takes on even greater importance. From ISTE

<https://www.iste.org/explore/how-states-can-support-next-generation-digital-citizens>):

- A. Digital citizenship empowers students to engage with the most culturally relevant problems of today. In the past year, we have observed numerous examples of technology used to raise awareness of ongoing social justice issues. At the same time, technology accelerated the sharing of misinformation about the pandemic. By helping students grow as digital citizens who use technology to facilitate the productive and equitable exchange of information and opportunity, rather than sow discord, we can empower them to engage with global challenges.
- B. Digital citizenship takes advantage of active uses of technology. Teachers note that one of the most significant challenges in the past year has been engaging students in the learning process. Digital citizenship allows students to engineer their own learning processes in two critical ways:
1. Equipping students with opportunities to carefully evaluate digital information and collaborate in inclusive ways.
  2. Providing students with greater autonomy to dive into issues of personal interest, supporting a continuous feedback loop that transforms and innovates the students’ learning journey
  3. Digital citizenship provides a means to further engage the community in students’ learning. One advantage of remote learning in the past year has been the increased involvement of parents and caregivers in students’ learning. Building on this momentum, [some districts](#) have begun exploring how to involve this broader, external community in students’ learning about digital citizenship and reinforce the competency from home.

**C. Action Plans - Digital Citizenship**

1. Review and enhance DCSD Digital Citizenship Curriculum in the following subjects:
  - a) Media Balance & Well Being



- b) Privacy & Security
    - c) Digital Footprint & Identity
    - d) Relationships & Communication
    - e) Cyberbullying, Digital Drama & Hate Speech
    - f) News & Media Literacy
  - 2. Library Media Specialists support instruction in Digital Citizenship in PK-Grade 6
  - 3. Annual Development of push-in program in Digital Citizenship in Grades 7-12
  - 4. TAs under direction of Library Media Specialist develop and teach curriculum in Digital Citizenship
  - 5. Presentations to Students, Student Forums, and Student Surveys
  - 6. Annual evaluation based on student, staff, and parent feedback.
- II. **Action Plan - Technology Skills** - Create a Progression of Essential Technology skills PK - 12 revising as technology skills are increased in students. Develop exposure, introductory, developing and mastery levels in each of the following areas:
- A. Basic Procedural Skills
  - B. Communication skills
  - C. Data Entry and Analysis
  - D. Digital learning Environments
  - E. Multimedia
  - F. Search Skills
  - G. Writing & Publishing
- III. **Action Plan - STEAM Curriculum** - Develop and implement grade appropriate curriculum in the following subjects:
- A. Coding,
  - B. Computational skills
  - C. Robotics
  - D. Computer Science
  - E. Maker space
  - F. Engineering process
  - G. Project based learning
- IV. **BUDGET:** In house salaries - \$82,000
- V. **TIMELINES:** Ongoing

**Goal 3: Enhance the Cybersecurity infrastructure to provide the safety and security of all while simultaneously bringing the world of learning to our students.**

- I. NYS EdLaw2-d provides “guidance to educational agencies and their third-party contractors on ways to strengthen data privacy and security to protect student data and annual professional performance review data. Cyber security must be an integral part of every

education organization's mandate. Students, teachers, and administrators all need access to the learning tools necessary to understand, detect, and avoid cyber threats they may encounter in their daily activities. To help us get to that point, analyzing possible data breaches is key to understanding how schools are targeted and what can be done to minimize information security risk factors. For hackers, schools are an ideal target because they are a goldmine of personal information that's rarely protected by the same level of cyber security practices

- II. DCSD has been working with our local RIC and BOCES to ensure an effective cyber security infrastructure is developed and maintained. The Data Protection Officer for DCSD is the superintendent who has appointed a DPO team and charged them with enhancing cybersecurity infrastructure. The following are the Action Steps DCSD has taken and is continuing to take in the years ahead:
  - A. CyberSecurity - Best Practices
    - 1. password protection, password changes, password complexity,
    - 2. Internet filtering and blocking sites
    - 3. MFA (Multi Factor Authentication) on all Staff Google accounts
    - 4. Training staff in computer security best practices including locking computers, spotting phishing, reviewing and enhancing privacy.
  - B. Cybersecurity Staff Training
    - 1. All staff participate in annual cybersecurity protection training
    - 2. EdLaw2-d awareness and compliance training provided throughout the year
  - C. EdLaw2-d Compliance
    - 1. 3rd Party Vendors - ensuring contracts with third party vendors adhering to the requirements of EdLaw2-d
    - 2. Software Inventory - develop, maintain and link to SW inventory
    - 3. Parents Bill of Rights - establish, maintain and communicate - link to parents bill of rights <https://www.dansvillecsd.org/Page/2692> and in Appendix
    - 4. Parent Complaint Form - establish, maintain and communicate - [Technology Parent Complaint Form](#)
    - 5. Incident Response Planning - DCSD developed a plan to respond swiftly to suspected incidents and training staff to react quickly to suspicious activity
    - 6. Disaster Recovery Plan - The district is developing disaster recovery plans to ensure swift resumption of district operations post technology disaster
      - a) District will work with B&G and Operations on merging all Safety and Security, emergency response plans and technology Incident Response and Disaster Recovery planning
  - D. Risk Assessment Planning - 4 year comprehensive plan with EduTech

### III. BUDGET:

- A. Salaries of IT Staff
- B. Professional Development - In house, staff salaries
  - 1. Conferences - curriculum budget: \$37,000, BOCES Coser 526 about

\$100,000 annually for all professional learning of which effective instructional technology is a part.

- a) Most conferences in cybersecurity through BOCES for little or no cost
- 2. Districtwide PD- \$37,000. BOCES supported professional learning
- C. Third Party contracts with vendors are ongoing and annual. District State Aided
  - 1. Software account: \$38,000. Building Level Textbook/Software funds

#### IV. Timeline

- A. Staff training is ongoing and annual.
- B. Password Changes - 3 to 6 months
- C. MFA - 2022
- D. Vendor Contracts and SW inventory ongoing
- E. Parents Bill of Rights and Complaint form - 2021 - monitored ongoing
- F. Incident response plan - BOE Approved in 2021
  - 1. Table top training 2021-22 and ongoing
  - 2. Integrate with other district emergency response plans - 2023
- G. Disaster Recovery Plans - 2022-23
- H. Risk Assessment Planning
  - 1. 2021-22 - NIST Assessment Review
  - 2. 2022-23 - Network Security Analysis
  - 3. 2023-24 - Phishing Exercise
  - 4. 2024-25 - Vulnerability Scanning CISA

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

- I. While this is not a new goal or initiative, it remains important to list maintaining and supporting the network and all that entails as an ongoing goal for at least the 2022-25 timeframe. The 1:1 is well established as DCSD began our 1:1 program in Grades 2-12 in 2014-15, and financing the 1:1 independent from SMART Bond funds is new and of imperative importance. In addition increased cybersecurity awareness and threats highlight the importance of enumerating all the district does to keep our technology infrastructure state of the art.
- II. **Action Plan - Ongoing Support of Instructional Technology 2022-25 - Leverage district funds to support:**
  - A. **Professional Learning.** Ensure that an annual plan for cybersecurity professional learning is deployed to staff. Compliance reports ensure participation
  - B. **Instructional Support** - Ensure needs of students with disabilities and ESL students are supported with technology as necessary to allow equitable access to curriculum,

instruction and assessment.

- C. **Device Management** - Collaborative planning to enhance and maintain functional to state-of-the-art device inventory
  - 1. Advise superintendent on SMART Bond Act and long term funding to support desktop replacement, and building capacity to support the 1:1 student:Chromebook program from district annual resources in collaboration with EduTech.
  - 2. Maintain funding for replacement of devices according to 1:1 Roadmap (See Appendix C) with SMART Bond funds through 2021 and transitioning to EduTech leases beginning in 2022
  - 3. 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. Remaining district SMART Bond allocation planned to be used for Desktop Replacement plan 2023 to 2025 timeframe.
- D. **Systems Management** - Ensure systems are functioning and continue to meet district operational needs. Assist in onboarding of new systems
  - 1. 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
  - 2. Maintain a single district-wide student records database solution (SchoolTool) with web access for students, parents and teachers, and Food Service and Transportation databases.
    - a) 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.
  - 3. 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) .
- E. **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.
  - 1. Monitoring of Website, Blackboard to promote Expanded and updated communication with school community.
  - 2. Use Blackboard Connect, website, and DCS App to allow customized voice messages to be efficiently delivered to DCS students, staff, parents and community.

III. **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 in the past provided 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. In 2022 - 2025, DCSD would use remaining funds to replace desktop computers. Federal ARPA Funds will be used to upgrade, replace and install Interactive Whiteboards to allow the engaging instructive technology that enhances student learning. DCSD will also leverage ECF to assist with providing Internet access 24/7 to our students. And finally eRate funds will be used to upgrade the network access points. 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. The Professional Learning budget is part of the district Curriculum and PD funds. Curriculum, Professional Learning and Technology provided under one administrator. 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. Any additional software would be funded through the district software budget and/or the Wayne-Finger Lakes Administration SAA.

**A. Overall Technology Budget**

1. EduTech Support:	\$ 731,000
2. Computer Equipment:	\$ 30,000
3. Computer Repairs	\$ 12,587
4. Computer Supplies	\$ 15,000
5. Software	\$ 37,759
6. ARPA Funds for Technology	\$125,000
7. 1:1 Roadmap annual expenses	\$130,000
8. SMART Bond	\$325,000

**B. Overall Professional Learning Budget (technology is an integral part of professional learning budget)**

1. Teacher Professional Learning	\$ 48,500
2. Curriculum & Professional Learning	
a) BOCES	\$187,500

**C. Salaries of staff support the DCSD Master Technology Plan**

## DCSD 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.

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 Spectrum. 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. Fiber connection to our District Office is leased through Empire Access. 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 - 1 gbps fiber (as of January 4, 2022 ), (Spectrum 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 Palo Alto VPN solution. On an "as needed" basis, 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 - Blackboard, including mass communication system and an app. Emphasis on ease of communication with community, social media, and mobile devices, the website enhances communication and collaboration with our community. 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 be 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, Teachers, & Educational Leaders**

**APPENDIX B: Technology Use Guide**

**APPENDIX C: 1:1 Road Map**

**APPENDIX D: Acceptable Use Policy (AUP)**

**APPENDIX E: FERPA Notification**

**APPENDIX F: Parent Bill of Rights**

**APPENDIX G: Code Of Conduct Documents**

**APPENDIX H: Technology Consultation and Collaboration**

## Appendix A: ISTE Standards for Students, Teachers and Educational Leaders:

### 1. [ISTE Standards combined 2021](#)

#### Technology Use Guide

### Appendix B: 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 annually.

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, nor permitted on the district network.

#### 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. Students 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 devices. 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 - See Appendix D

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 of the District at any time. Unsupervised Chromebooks or other district issued electronic devices 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 devices 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 devices 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 email 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 email.

## 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 emails.

## 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.

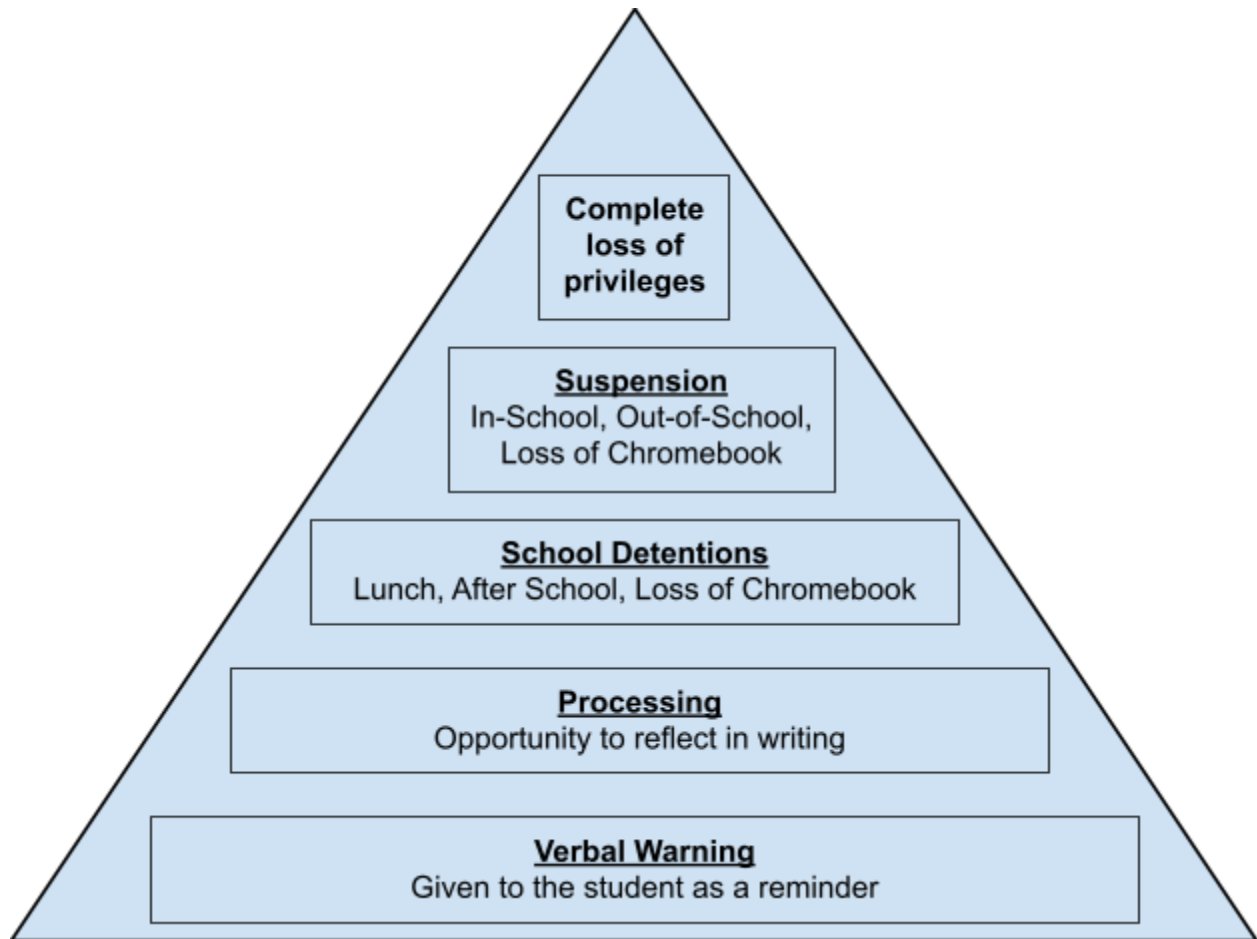
1. The Technology Discipline Hierarchy applies to all DCSD technology, not just Chromebook computers. This includes, but is not limited to iPads, SMARTBoards, Promethean Boards, document cameras, projectors, desktop computers, printers, mice, digital cameras, etc.
2. Discipline is progressive. Low-level, 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 devices 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 devices, 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 devices 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 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 devices, chargers and cases. Chromebooks or other district issued electronic devices 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 devices 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 devices 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 C: 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:

	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27	Symbol
2019	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	Acer 8-2014
2020	Asus 7-2018	XXX	XXX	XXX	XXX	XXX	XXX	XXX	Asus 12-2016
2021	Asus 7-2018	Asus 7-2018	XXX	XXX	XXX	XXX	XXX	XXX	Asus 9-2017
2022	SB3 CTL	SB3 CTL	SB3 CTL	XXX	XXX	XXX	XXX	XXX	Lenovo N23T
2023	Asus 9-2017	SB6 CTL	SB6 CTL	SB6 CTL	XXX	XXX	XXX	XXX	Asus 7-2018
2024	Asus 7-2018	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL	XXX	XXX	XXX	2019-20 Smart Bond 3
2025	SB3 CTL	SB3 CTL	SB3 CTL	2022-23 New	2022-23 New	2022-23 New	XXX	XXX	2020-21 Smart Bond 6
2026	Asus 12-2016	SB6 CTL	SB6 CTL	NEW	2023-24 New	2023-24 New	2023-24 New	XXX	2021-22 New
2027	Asus 9-2017	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL	2024-25 New	2024-25 New	2024-25 New	2021-22 New 2nd Grade
2028	Asus 7-2018	SB6 CTL	SB6 CTL	2022-23 New	2022-23 New	2022-23 New	2025-26 New	2025-26 New	2022-23 New
2029	SB3 CTL	SB3 CTL	SB3 CTL	NEW	2023-24 New	2023-24 New	2023-24 New		2023-24 New
2030	Lenovo N23T	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL	2024-25 New	2024-25 New	2024-25 New	2024-25 New
2031	XXX	Lenovo N23T	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL	2025-26 New		2025-26 New
2032	XXX	XXX	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL	SB6 CTL		2026-27 New
2033	XXX	XXX	XXX	NEW	2023-24 New	2023-24 New	2023-24 New	2023-24 New	
2034	XXX	XXX	XXX	XXX	New 2nd grd	2024-25 New	2024-25 New	2024-25 New	
2035	XXX	XXX	XXX	XXX	XXX	New 2nd grd	2025-26 New		
2036	XXX	XXX	XXX	XXX	XXX	XXX	New 2nd grd	2026-27 New	

## **APPENDIX D:**

# **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 of 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 E:

### 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 E: Parent Bill of Rights

# Dansville Central School District Parents' Bill of Rights for Data Privacy and Security

The Dansville Central School District is committed to ensuring student privacy in accordance with local, state and federal regulations and district policies. To this end and pursuant to U.S. Department of Education (DOE) regulations (Education Law §2-d), the district is providing the following Parents' Bill of Rights for Data Privacy and Security:

- A student's personally identifiable information cannot be sold or released for any commercial or marketing purposes.
- Parents have the right to inspect and review the complete contents of their child's education record, including any student data maintained by the Dansville School District. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record. The New York State Education Department (SED) will develop further policies and procedures related to these rights in the future.
- State and federal laws protect the confidentiality of personally identifiable information 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.
- A complete list of all student data elements collected by the state is available for public review in an Excel file at <http://www.nysed.gov/data-privacy-security>. Parents may also 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, N.Y. 12234.
- Parents have the right to have complaints about possible breaches of student data addressed.
  - Complaints should be directed to: Superintendent of Schools, Dr. Paul J. Alioto, 337 Main Street, Dansville, NY 14437.
  - Complaints to SED should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; the e-mail address is [cpo@mail.nysed.gov](mailto:cpo@mail.nysed.gov).
  - Or complete this form: **PARENT DATA COMPLAINT FORM**

We are compiling the following information about each agreement between DISTRICT and an outside party that receives protected student data, or protected principal or teacher data, from the district: (1) the exclusive purposes for which the data will be used,

(2) how the contractor will ensure that any subcontractors it uses will abide by data protection and security requirements, (3) when the contract expires and what happens to the data at that time, (4) if and how an affected party can challenge the accuracy of the data, (5) where the data will be stored, and (6) the security protections taken to ensure that data will be protected, including whether the data will be encrypted. The links below will take you to the list of vendors. We will be updating this list as we gather additional information.

[DCSD Third Party Vendor List](#)

**APPENDIX F: Code of Conduct Documents**  
**Reference Codes of Conduct of all buildings**  
[HS Code of Conduct](#)  
[EBH Code of Conduct](#)

**APPENDIX J: Technology Committee and Collaborators**

Member	Title	Email
Dr. Paul Alioto	DCSD Superintendent	aliotop@dansvillecsd.org
Lynne Blum	HS Library/Media Specialist	bluml@dansvillecsd.org
Joie Petrillo	DCSD PS	petrilloj@dansvillecsd.org
John Leuzzi	DCSD IT Specialist	leuzzij@dansvillecsd.org
Kim Derrenbacher	Tech PD and District PR	measek@dansvillecsd.org
Mike Birmingham	DCSD Network Administrator	birmingham@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 Allen	EBH Principal	allenl@dansvillecsd.org
DCSD Shared Decision Making Team		