

8/4/26 SPECIAL BOARD MEETING
Tuesday, August 4, 2026 6:00 PM Eastern

HS LGI Room
700 New School Lane
Dallastown, PA 17313

Wesley Anderson:	Present
Dina Aubel:	Present
Matthew Charvat:	Present
James Cohn:	Present
Karl Dotterweich:	Present
Albert Granholm (Dallastown):	Present
Anthony Pantano:	Present
Eric Pierce:	Present
Scott Wingard:	Present

Present: 9.

1. **PLEDGE OF ALLEGIANCE - Mr. Pantano**
2. **ROLL CALL & EXECUTIVE SESSION ANNOUNCEMENT - Mr. Pantano**
3. **APPROVAL OF BOARD AGENDA**
4. **COMMENTS FROM THE PUBLIC**
5. **PROCEDURAL REVIEW - Mr. Pantano**
6. **CELLPHONE PARAMETERS**
7. **STUDENT DEVICE PARAMETERS**
8. **K-3 TOILETING**
9. **CALENDAR OF BOARD EVENTS**
10. **COMMENTS FROM THE PUBLIC**
11. **BOARD COMMENTS / CORRESPONDENCE**
12. **ADJOURNMENT**

Dallastown Area School District

Policy 815.1 — Acceptable Use of Personal Technology Devices

Printed 6/30/2026

Policy Number 815.1

Title Acceptable Use of Personal Technology Devices

Adopted 6/13/2013

815.1

Acceptable Use of Personal Technology Devices

📅 Adopted: 6/13/2013

Purpose

Dallastown Area School District is committed to the use of technology in supporting both the instructional program and district business operations. Dallastown Area School District is also committed to protecting student, employees, and stakeholders from illegal, inappropriate, and damaging technology use by individuals, either knowingly or unknowingly. It is the purpose of the policy to define the appropriate use of personal technology within Dallastown Area School District buildings and sponsored events.

Definition

Personal technology devices shall include all devices that can take photographs; record audio or video data; store, transmit or receive messages, images or other data; or provide wireless, unfiltered connection to the Internet.

Examples include digital video and audio recorders, e-readers, laptop computers, smart phones, iPads, netbooks, as well as any new technology developed with similar capabilities.

Guidelines

Employees – Personal Devices

The district's technology services department will make every attempt to provide all necessary devices required for the educational and business needs of the district. However, there may be circumstances where this is not possible or practical. The use of personal technology devices on school property is permissible for educational purposes or school business during school hours. In such instances, employees shall abide by the following terms:

1. To be compliant with Child Internet Protection Act laws for filtering, personal technology devices used to access Internet for instructional or presentation purposes must do so through the identified district wireless network.
2. The user of a personal technology device found to be the source of an intended virus, worm, trojan horse, spyware, or other malicious software on the district network can be held liable for all resulting damages to district technology resources.
3. Accessing, creating or sending inappropriate content stored on personal technology devices while on district property or at school-related events constitutes a violation of the Acceptable Use of Technology Resources Policy (AUP) and is subject to the consequences thereof.[1]
4. Employee assumes all responsibility for the safety of all content on personal technology devices. Employees should avoid keeping any district and/or student personal identification information on personal devices. In case it is essential to have this information on personal devices, employees are responsible to maintain an accurate, up-to-date inventory of any district file or data that could contain personal identification information.
5. The Dallastown Area School District reserves the right to examine personal technology devices on district premises which are regularly used for instructional purposes when the district has a reasonable basis to suspect that an employee violated this policy. Access to material or communications on the device may be required as part of the Right-to-Know Law, if such material or communications constitute a public record of the district.
6. The district shall not be liable for the loss, damage, or misuse of any personal technology devices.

Consequences for Inappropriate Employee Use

Failure to follow the procedures and prohibitions listed above may result in the loss of the right to use personal technology devices, loss of access to network resources, and appropriate disciplinary action up to and including termination of employment. Illegal use of the personal technology device, for example intentional deletion or damage to files or data belonging to others, copyright violations or theft of services, may be reported to the appropriate legal authorities for possible prosecution.[2][3][4]

Students – Personal Devices

Personal technology devices may be used by students during the school day for educational purposes, under the following conditions and within the procedures defined by the building administrator:

1. Students may use personal technology devices during the school day while either on district property or attending off-site school-sponsored activities if the use is for educational purposes and the student has permission, as defined by the building administrator.
2. Students using personal devices to take photographs or to record audio or video during the school day must have appropriate permission, as defined by the building administrator. Any student using the device to photograph or record audio or video, which determined in the sole discretion of the building administrator is used to embarrass, harass, or intimidate another, may face appropriate legal and disciplinary consequences.
3. Personal technology devices cannot be used to compromise the integrity of any component of the instructional program (e.g. electronic cheating, plagiarism, recording audio and video without permission, posting of inappropriate content not related to instructional activities).
4. The user of a personal technology device found to be the intended source of a virus, worm, trojan horse, spyware, or other malicious software on the district network can be held liable for all resulting damages to district technology resources.
5. Accessing, creating or sending inappropriate content stored on personal technology devices while on school property or at school-sponsored events constitutes a violation of the Acceptable Use of Technology Resources Policy (AUP) and is subject to the consequences thereof.[1]
6. Personal technology devices brought into school are to supplement instructional activities and must be used in accordance to the guidelines identified by the building administrator. Students must receive appropriate permission to bring such devices into the district by the building administrator in consultation with the Technology Services Department. Such devices are permitted to be connected through the identified district wireless network.
7. The Dallastown Area School District reserves the right to examine all personal technology devices at any time that the district has reasonable basis to suspect that the student is not complying with this policy.
8. The district shall not be liable for the loss, damage, or misuse of any personal technology devices while on district property or while attending school-sponsored activities.

Consequences for Inappropriate Student Use

Violations of this policy by a student may result in disciplinary action and the confiscation of the electronic device. Confiscated items may be returned at the principal's discretion. Violations may also result in student not being allowed to use personal technology devices and loss of district network privileges.

Footnotes

[1] **Pol. 815** *Policy reference not found*
Policy Reference

[2] **Pol. 317** *Policy reference not found*
Policy Reference

[3] **Pol. 417** *Policy reference not found*
Policy Reference

[4] **Pol. 517** *Policy reference not found*
Policy Reference

CELL PHONE Expectations

Grades K-3

"Off and Away" at all times.

Not permitted, unless directed by staff.

1st Offense: Confiscate phone; student pick-up at end of day. parent contact required.

2nd Offense: Parent pick-up required; student assigned detention.

3rd Offense: Parent pick-up required; student assigned detention and cell phone ban.

Subsequent Offenses: Consequences may include suspension if usage is inappropriate.

Grades 4-6

"Off and Away" at all times.

Not permitted, unless directed by staff. Zero tolerance for in-school social media posting.

1st Offense: Confiscate phone; student pick-up at end of day. parent contact required.

2nd Offense: Parent pick-up required; student assigned detention.

3rd Offense: Parent pick-up required; student assigned detention and cell phone ban.

Subsequent Offenses: Consequences may include suspension. Social media posting during school hours will result in confiscation of phone, guardian phone call, 1-3 days lunch detention, and/or in-school suspension.

CELL PHONE Expectations

Grades 7-8

"Off and Away" at all times.

Permitted only for a specific educational purpose under teacher supervision.

1st Offense: Confiscate phone until 2:50 PM. Warning logged in Skyward; Parent contact.

2nd Offense: Confiscate phone until 2:50 PM. Referral logged in Skyward; Office assigns Detention.

3rd Offense: Same as 2nd offense (Referral + Detention).

Repeated offenses lead to escalation via the main office (Detention/In-School Suspension).

Grades 9-12

Prohibited during direct instruction.

Permitted in hallways, study halls, and at lunch. Teacher may allow use during self-directed work.

1st Offense: Teacher warning.

2nd Offense: Teacher warning and contact home.

3rd Offense: Teacher-assigned detention.

Subsequent Offenses: Office referral (leading to office-assigned consequences).

Dallastown Area School District

Policy 815 — Acceptable Use of Technology/Internet

Printed 6/30/2026

Policy Number	815
Title	Acceptable Use of Technology/Internet
Adopted	12/7/2000
Revised	4/23/2026

815

Acceptable Use of Technology/Internet

📅 Adopted: 12/7/2000 📅 Last Revised: 4/23/2026

Purpose

The Board supports the use of technology devices and Internet in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of technology devices and network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities and developmental levels of students.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: [\[1\]](#)

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
3. Such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.[\[2\]](#)

Computer - for purposes of this policy, district computers include any electronic device owned or leased by the district that has the capability to create, play or edit text, audio and video data; transmit or receive messages, text, data or images; operate software or online applications; or provide a wired or wireless connection to the Internet.

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[\[3\]](#)[\[4\]](#)

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
2. Depicts, describes or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and
3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement or sadomasochistic abuse, when it:[\[5\]](#)

1. Predominantly appeals to the prurient, shameful or morbid interest of minors;
2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance, if: [\[5\]](#)

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;
2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors. [\[4\]](#)

Network facilities - the district's computers, tablets, cell phones, electronic communication systems and network, which includes Internet access, whether wired or wireless.

Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Emergent Technologies - new and evolving digital tools, applications, and platforms, including but not limited to artificial intelligence, machine learning, virtual/augmented reality, generative media, wearable technology, biotechnology, cloud services, quantum computing, nano/macrotechnology, and related systems that impact teaching, learning, and operations.

AI literacy - the ability to understand, use and interact with AI systems effectively, efficiently and responsibly.

Technology Literacy - the ability to understand, use, and interact with emergent technologies effectively, efficiently, and responsibly.

Open-source Tools - publicly accessible emergent technology platforms that may share user data broadly.

Artificial Intelligence (AI) - technology designed to mimic human intelligence, such as analyzing data, recognizing patterns and making decisions.

Generative Artificial Intelligence (Generative AI) - an advanced subset of AI that is capable of generating new content from learned data and pattern recognition across various mediums such as text, code, images, audio and video data. Generative AI is the focus of this policy.

Open-source AI - AI tools and resources that are built on publicly accessible platforms and use and share data among all users who access the platform, both within and outside of the district.

Authority

The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board declares that district internet, computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, access, receive or display on or over the district's Internet, computers or network resources, including personal files. The district reserves the right to monitor, track and log network access and use on district computers and network resources; monitor fileserver space and file storage utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.[6][7][8][9][10]

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the building principal or designee.

The Board establishes the following list of subject areas as inappropriate matter, in addition to those stated in law and defined in this policy, which shall not be accessed by minors or created or generated by any user of the district's computers and network resources: [\[4\]](#).

1. Lewd, vulgar or profane materials.
2. Threatening materials. [\[11\]](#)[\[12\]](#)
3. Harassing or discriminatory. [\[13\]](#)[\[14\]](#)[\[15\]](#)
4. Bullying. [\[16\]](#)
5. (Consisting of/Relating to) Weapons. [\[17\]](#)
6. Terroristic. [\[18\]](#)

The district reserves the right to restrict access to any Internet sites or network functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking/filtering. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers and network resources used and accessible to adults and students. The technology protection measure shall be enforced during use of computers and network resources with Internet access. [\[3\]](#)[\[4\]](#)[\[19\]](#)

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the adjustment of technology protection measures to enable access to material that is blocked or filtered but is not prohibited by this policy. [\[19\]](#)

Upon request by students or staff, building administrators may authorize the temporary adjustment of technology protection measures to enable access to otherwise prohibited materials for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to adjusting Internet blocking/filtering for a student's use. If a request for temporary adjustment of technology protection measures is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review. [\[3\]](#)[\[20\]](#)

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[\[19\]](#)

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Generative AI and Emerging Technology tools and resources used in district schools and programs shall be evaluated and authorized on an ongoing basis for age-appropriateness, bias, privacy protections, accessibility standards and data security by the Director of Technology Services, the Director(s) of Educational Services, or designee.

The Board directs that only district-authorized Generative AI and Emerging Technology tools and resources may be used on district computers and in district schools and programs. Staff shall consult the district's list of authorized Generative AI and Emerging Technology tools and resources prior to implementation in the educational environment. Unauthorized Generative AI and Emerging Technology tools and resources may not adhere to required data privacy, monitoring and security standards.

Student user agreements shall also be signed by a parent/guardian.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Building principals shall make initial determinations of whether inappropriate use has occurred, and may consult with the Superintendent or designee and the school solicitor when necessary.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers and network resources are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[\[3\]](#)[\[4\]](#)[\[21\]](#)

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors or determined inappropriate for use by minors by the Board.
2. Maintaining and securing a usage log.
3. Monitoring online activities on district computers and network resources.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[\[4\]](#)

1. Interaction with other individuals on social networking websites and in chat rooms.
2. Cyberbullying awareness and response.[\[16\]](#)[\[22\]](#)

AI Literacy

Staff –

The district shall provide staff with professional development opportunities addressing the effective and safe integration of Generative AI and Emerging Technology to enhance teaching and learning. Professional development opportunities may include, but not be limited to:

1. Ethical use of Generative AI and Emerging Technology.
2. The capabilities and limitations of Generative AI and Emerging Technology.
3. Critical analysis of content produced by Generative AI and Emerging Technology.
4. How to monitor and evaluate student inputs into Generative AI and Emerging Technology systems.
5. The parameters established by the district for integrating Generative AI and Emerging Technology tools into classroom instructional design.

Beyond formal professional development opportunities, the district encourages staff to explore Generative AI to discover lesson plan ideas, create templates or assessments and to generate ideas for the personalization of student learning. Generative AI and Emerging Technology tools and resources shall be used in accordance with applicable laws,

regulations and this Board policy.

Students –

The district shall provide training for students, which may include, but not be limited to:

1. Establishment of expectations regarding the ethical use of Generative AI and Emerging Technology.
2. The capabilities and limitations of Generative AI and Emerging Technology.
3. Critical analysis of content produced by Generative AI and Emerging Technology.
4. How to disclose use and cite Generative AI and Emerging Technology resources.
5. The importance of not disclosing personally identifiable information when using an open-source Generative AI and Emerging Technology tools or resources.

Guidelines

District computers and network accounts shall be used only by the authorized user of the computer or account for its approved purpose. Network users shall respect the privacy of other users on the system.

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher, building administrator or other appropriate school staff. Network users shall not reveal personal information to other users on the network or Internet, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[\[4\]](#)[\[21\]](#)

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, social networking websites and other forms of direct electronic communications.

3. Prevention of unauthorized online access by minors, including hacking and other unlawful activities.
4. Unauthorized disclosure, use and dissemination of personal information regarding minors.[23][24][25]
5. Restriction of minors' access to materials harmful to them or which have been designated as inappropriate matter in Board policy.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with Board policy, accepted rules of network etiquette and federal and state law and regulations. Specifically, the following are prohibited uses of district computers and/or network resources:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.
4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[16][22]
6. Discriminatory remarks, harassment and offensive or inflammatory communication. [13][14][16][26]
7. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials.[27]
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd or otherwise illegal materials, images or photographs.[34]
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
10. Vulgar language or profanity.
11. Transmission of material that a reasonable person would know to be offensive or objectionable to recipients.

12. Intentional obtaining or modifying of files, passwords and data belonging to other users.
13. Impersonation of another user, anonymity and pseudonyms.
14. Fraudulent copying, communications or modification of materials in violation of copyright laws.[27]
15. Loading or accessing unauthorized games, programs, files or other electronic media.
16. Disruption of the work of other users.
17. Destruction, modification, abuse or unauthorized access to network hardware, software, systems and files.
18. Accessing the Internet, district computers or other network resources without authorization.
19. Disabling, adjusting or bypassing the Internet blocking/filtering technology protection measure(s) without authorization.
20. Accessing, sending, receiving, transferring, viewing, sharing, deleting or downloading confidential information without authorization.

The district prohibits the use of Generative AI and Emerging Technology in making decisions regarding employee recruitment, hiring, retention, promotion, transfer evaluation, demotion or dismissal.

The district prohibits the use of Generative AI and Emerging Technology in making final determinations on student assessments and evaluations.

Security

System security is protected through the use of passwords and/or encryption and district security procedures. Failure to adequately protect passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:[25][28][29]

1. Employees, students and other authorized users shall not reveal their passwords to another individual with the exception of a parent/guardian.
2. Users are not to use a computer that has been logged in under another user.

3. Any user identified as a security risk or having a history of problems with other computers or network systems may be denied access to the district's computers and network resources.

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network or Internet shall be subject to fair use guidelines and applicable laws and regulations.[27][30]

District Website

The district may establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All authorized users publishing content on the district website shall receive appropriate training and comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

Accessibility –

District staff who maintain district websites and web pages shall post content which is accessible to individuals with disabilities, to the same extent that it is available to other users, based on the needs of the individuals and limitations of the platform. This shall include, but is not limited to:[13][14][15][31][32][33]

1. Including alternate text descriptions or captions for images.
2. Including captions for video content.
3. Avoiding text that is posted as an image or conveyed using only color cues.
4. Creating links and attachments in formats that are accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.
5. Formatting text so that it is accessible to screen readers and other assistive technology, and may be accessed through keyboard or speech navigation.

All district websites shall contain clear contact information that may be used by members of the public to request accommodations or assistance.

Academic Integrity

Emerging Technology tools should supplement the educational process without undermining the integrity of academic work. Examples of appropriate use may include, but are not limited to, generating ideas for brainstorming sessions, providing tutoring in specific subjects, and automating administrative tasks.

The use of AI, Generative AI or other Emerging Technology by students to complete assignments or assessments shall only be allowed to the extent stated and outlined by the teacher for the individual assignment or course. Should AI tools be permitted, students shall be notified in advance of the parameters for the use of AI, Generative AI or other Emerging Technology in assignments and assessments.

Direct submission of AI-generated or Emerging Technology-generated work as one's own without proper attribution or reliance on the same for completing assignments and/or without understanding the content is prohibited.

Users must respect copyright laws and intellectual property rights when using AI tools. This includes not using AI, Generative AI or other Emerging Technology to replicate or modify copyrighted materials without authorization and properly citing all sources of content, including AI-generated content, to avoid plagiarism. Should students be permitted to utilize AI tools for such an assignment, usage must be cited.

Consequences for Inappropriate Use

Users of district computers and network resources shall be responsible for damages to the equipment, systems, platforms and software resulting from deliberate or willful acts. [\[19\]](#)

Illegal use of the district computers and network resources; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules and Board policies for behavior and communications apply when using the district computers, network resources and Internet, in addition to the stipulations of this policy.

Vandalism shall result in loss of access privileges, disciplinary action and/or referral to legal authorities. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, the district, the Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action and/or referral to legal authorities.[6][7][8][9][10]

Footnotes

[1] 18 U.S.C. 2256
law.cornell.edu [View source](#)
law.cornell.edu

[2] 18 Pa. C.S.A. 6312
palegis.us [View source](#)
palegis.us

[3] 20 U.S.C. 7131
uscode.house.gov [View source](#)
uscode.house.gov

[4] 47 U.S.C. 254
law.cornell.edu [View source](#)
law.cornell.edu

[5] 18 Pa. C.S.A. 5903
palegis.us [View source](#)
palegis.us

[6] Pol. 218 *Policy reference not found*
Policy Reference

[7] Pol. 233 *Policy reference not found*
Policy Reference

[8] **Pol. 317** *Policy reference not found*
Policy Reference

[9] **Pol. 417** *Policy reference not found*
Policy Reference

[10] **Pol. 517** *Policy reference not found*
Policy Reference

[11] **24 P.S. 1302-E**
palegis.us [View source](#) 
palegis.us

[12] **Pol. 236.1** *Policy reference not found*
Policy Reference

[13] **Pol. 103** *Policy reference not found*
Policy Reference

[14] **Pol. 104** *Policy reference not found*
Policy Reference

[15] **Pol. 103.1** *Policy reference not found*
Policy Reference

[16] **Pol. 249** *Policy reference not found*
Policy Reference

[17] **Pol. 218.1** *Policy reference not found*
Policy Reference

[18] **Pol. 218.2** *Policy reference not found*
Policy Reference

[19] **24 P.S. 4604**
palegis.us [View source](#) 
palegis.us

[20] **24 P.S. 4610**
palegis.us [View source](#) 
palegis.us

[21] **47 CFR 54.520**
law.cornell.edu [View source](#) 
law.cornell.edu

[22] **24 P.S. 1303.1-A**
palegis.us [View source](#) 
palegis.us

[23] **Pol. 113.5** *Policy reference not found*
Policy Reference

[24] **Pol. 216** *Policy reference not found*
Policy Reference

[25] **Pol. 830** *Policy reference not found*
Policy Reference

[26] **Pol. 247** *Policy reference not found*
Policy Reference

[27] **Pol. 814** *Policy reference not found*
Policy Reference

[28] **Pol. 800** *Policy reference not found*
Policy Reference

[29] **Pol. 830.1** *Policy reference not found*
Policy Reference

[30] **17 U.S.C. 101**
law.cornell.edu [View source](#) 
law.cornell.edu

[31] **42 U.S.C. 12101**
law.cornell.edu [View source](#) 
law.cornell.edu

[32] **29 U.S.C. 794**
law.cornell.edu [View source](#) 
law.cornell.edu

[33] **28 CFR 35.160**
law.cornell.edu [View source](#) 
law.cornell.edu

[34] **Pol. 237** *Policy reference not found*
Policy Reference

K-6 Student Device Usage Summary



Discussion: K-6 district device restrictions 11 PM – 6 AM

Student Devices K-6

- One-to-One Chromebooks
 - K-3: district devices are sent home as needed
 - 4-6: district devices are sent home daily for most students

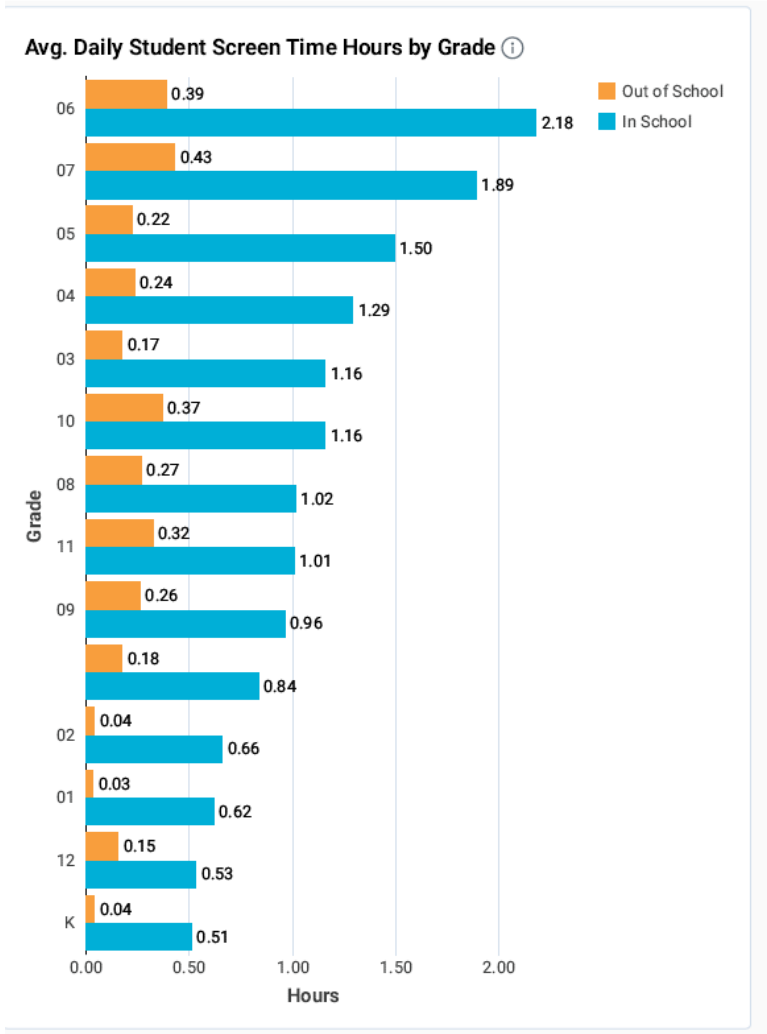
Key considerations:

- Restrictions can be time-based or location-based using after-school rule sets.
- Only one after-school rule set can be active at a time.
- Rules can be applied by grade level or building.
- We currently use these settings to support after-hours student activities, such as eSports access, while limiting access during the school day.
- K-3 devices would generally not be impacted, as they are not taken home except during FID/Virtual days.
- Evening internet usage is lower, but some students are still actively using district devices to complete schoolwork due to work or extracurricular activities.

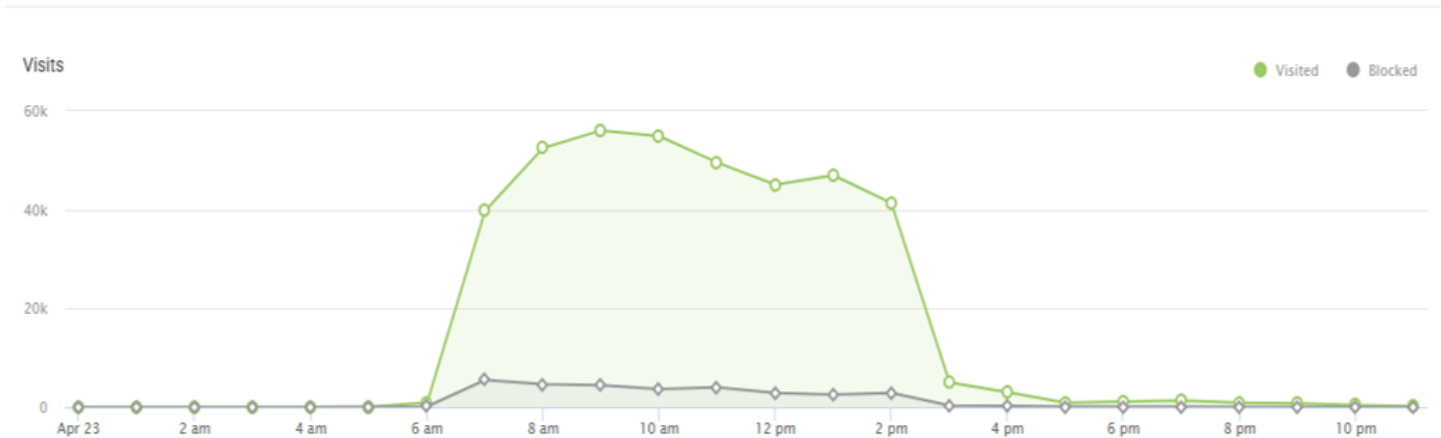
Notable Highlights:

- **1.19** average daily In-school hours
- **0.24** average daily out-of-school hours
- **Similar Organizations** – in-school daily hours **1.32** vs. our **1.19**
- **Similar Organizations** – out-of-school daily hours is **0.26** vs. our **0.24**

Usage Data Report (2022-2026 - all campuses)



Internet Overview



Dallastown Area School District

Policy 200 — Enrollment in District

Printed 7/9/2026

Policy Number	200
Title	Enrollment in District
Adopted	10/6/2005
Revised	5/16/2024

200

Enrollment in District

📅 Adopted: 10/6/2005 📅 Last Revised: 5/16/2024

Authority

The Board shall enroll school age students eligible to attend district schools, in accordance with Board policy, laws and regulations.[\[1\]\[2\]\[3\]\[4\]\[5\]\[6\]](#)

Definitions

School age shall be defined as the period from the earliest admission age for the district's kindergarten program until graduation from high school or the end of the school term in which a student reaches the age of twenty-one (21) years, whichever occurs first.
[\[1\]\[7\]](#)

District of residence shall be defined as the school district in which a student's parents/guardians reside.[\[2\]\[5\]](#)

Guidelines

Enrollment Requirements

A school age student shall be entitled to attend the schools of the district of residence if enrollment capacity permits.[\[1\]\[2\]\[5\]\[8\]\[9\]](#)[\[10\]](#)

The district shall enroll a school age, eligible student the next business day, but no later than five (5) business days after application.

The district shall not enroll a student until the parent/guardian has supplied proof of the student's age, residence, and immunizations required by law and regulations, except as follows:

1. Students Experiencing Educational Instability -

The district shall immediately enroll students experiencing homelessness, foster care and other forms of educational instability, even if the student or parent/guardian is unable to produce the required documents, in accordance with Board policy, law and regulation.[\[4\]](#)[\[11\]](#)

2. Children of Active Duty Military Families -

The district shall facilitate the timely enrollment and permit advanced enrollment of children of active duty military families, in accordance with law and Board policy. To qualify for advanced enrollment, prior to establishing residency in the district, a copy of the official military orders shall be provided to the district along with proof of the parent's/guardian's intention to move into the district. The parent/guardian must provide proof of residency within forty-five (45) days after the arrival date stated in the military orders.[\[3\]](#)[\[12\]](#)[\[13\]](#)

The district shall not inquire about the immigration status of a student as part of the enrollment process.[\[5\]](#)

Enrollment requirements and procedures shall apply to nonresident students approved to attend district schools, in accordance with Board policy, by the Superintendent.

The district shall administer a home language survey to all students enrolling in district schools for the first time.[\[5\]](#)[\[14\]](#)

Residency Eligibility

When the parents/guardians of a student reside in different school districts, the student may attend school in the district of residence of the parent/guardian with whom the student lives for a majority of the time, unless a court order or court approved custody agreement specifies otherwise.

If the parents/guardians of a student share joint custody and time is evenly divided, the parents/guardians may choose which of the two (2) school districts the student will enroll in for the school year.

If the student is an emancipated minor, the resident school district shall be the one in which the student is then living.

Footnotes

[1] 24 P.S. 1301 [View source](#) 

[2] 24 P.S. 1302 [View source](#) 

[3] 24 P.S. 1302.1 [View source](#) 

[4] 24 P.S. 1331.1 [View source](#) 

[5] 22 PA Code 11.11 [View source](#) 

[6] 22 PA Code 11.41 [View source](#) 

[7] 22 PA Code 11.12 [View source](#) 

[8] 24 P.S. 1302.1-A [View source](#) 

[9] 22 PA Code 12.1 [View source](#) 

[10] Pol. 202
Policy Reference [Open policy](#) 

[11] Pol. 251
Policy Reference [Open policy](#) 

[12] 24 P.S. 7302 [View source](#) 

[13] Pol. 254
Policy Reference [Open policy](#) 

[14] Pol. 138

Policy Reference

[Open policy](#)



Dallastown Area School District

Policy 200-AR-0 — Enrollment of Students

Printed 7/9/2026

Policy Number	200-AR-0
Title	Enrollment of Students
Adopted	3/16/2020
Revised	5/16/2024

200-AR-0

Enrollment of Students

📅 Adopted: 3/16/2020 📅 Last Revised: 5/16/2024

Pennsylvania resident students are considered school age and are entitled to attend district schools from the time they are admitted to a public school until graduation from high school or the end of the school year in which they turn age twenty-one (21).

When a student of school age is presented by a parent/legal guardian to any district school for enrollment, school staff will require the following documentation:

1. Proof of the student's age – acceptable documentation includes one (1) of the following: birth certificate; baptismal certificate; transcript of the record of baptism duly certified and showing the date of birth; notarized statement from the parents/guardians indicating date of birth; a valid passport; or a prior school record indicating the date of birth.
2. Immunization record with dates or assurance from the former school district or a medical office that the required immunizations have been completed or a required series has begun, with a record to be sent. Written statements are required for religious and medical exemptions.
3. Proof of residency – acceptable documentation includes one (1) of the following: deed; mortgage agreement; rent payment receipts or lease and one (1) of the following: PA driver's license or identification card; PA vehicle registration; property tax payment receipts; utility bill with current address; paycheck stub with employer and employee's address; or current voter registration.
4. Parental Registration Statement attesting to whether the student has been or is suspended or expelled for offenses involving drugs or alcohol, weapons, violence or conviction or adjudication for sexual assault against a student in the same school, as required by the Pennsylvania School Code.

School staff may ask for any of the following information, in addition to the required documentation, but will not require it as a condition of enrollment and will not delay a student's enrollment or attendance until the document(s) is provided:

1. Picture identification.
2. Health or physical examination records.
3. Academic records.
4. Attendance records.
5. Individualized Education Program or other special education records.
6. Registration form.

School staff will not request any of the following information to verify enrollment or residency:

1. Social security number.
2. Reason for a student's placement if not living with natural parent.
3. Visa of student or parent/guardian.
4. Student's immigration status.
5. Agency records.
6. Court order or records relating to a dependency proceeding, except in limited circumstances that occur when a custody order, agreement or dependency is being relied upon as the basis for enrollment.

District staff will consider what residency verification is reasonable in light of a family's situation and should be flexible.

The district will normally enroll a school age, eligible student the next business day, but no later than five (5) business days after application.

Upon enrollment of a student, school staff will contact the student's former school for a copy of the student's education records and disciplinary record, if any. If the school is within Pennsylvania, the disciplinary record should be sent within ten (10) business days.

The district cannot deny or delay a student's enrollment based on the information contained in a disciplinary record or sworn statement. However, the district can provide alternative education services during the period of expulsion for a student currently expelled for a weapons offense or conviction or adjudication for sexual assault against a person in the same school. If a student has been expelled from the previous district for reasons other than a weapons offense or conviction or adjudication for sexual assault against a person in the same school, the district will review the student's prior performance and school record to determine the services and supports that will be provided upon enrollment in the district.

Health records must be transferred from all public and private schools, upon the request of the building principal or designee.

The district will administer the home language survey to all students enrolling in the district for the first time.

The building principal will report to the Superintendent or designee the name of any student attempting to enroll who does not present the required documentation.

Students Enrolling Without Previous School Records

If a student is presented for enrollment without previous school records or if a private school withholds an enrolling student's records, the building principal may seek and accept information for student placement that appears reliable as proof of successfully completed coursework, such as report cards and sworn affidavits of previous school teachers.

If reliable information cannot be obtained, the building principal, in consultation with the appropriate staff, will promptly evaluate the student and determine the appropriate grade and/or courses for that student. The evaluation will consist of an interview and demonstration of the degree to which the student has achieved the academic standards established by the Board for district students.

The student and parents/guardians will be informed in writing of the results of the evaluation and the student's placement. The Board's adopted graduation requirements and planned instruction will be the criteria used by the school to determine a student's attainment of academic standards for high school graduation.

Change of Address

When a student or parent/guardian notifies District Enrollment of a change of address within the district's boundaries, the parent/guardian will be required to bring proof of residence to District Enrollment.

New student information will be modified on the Student Information System with the student's name, date of birth, new address, telephone number, school attending and grade.

The documentation accepted as proof should be noted on the registration form, and a copy of the document retained.

Enrollment Complaints

If a dispute involving enrollment arises, the concern shall be addressed and/or resolved at the lowest appropriate level in accordance with Board policy. (Pol. 906)

Enrollment disputes regarding students experiencing homelessness, foster care and other educational instability will be handled in accordance with Board policy. (Pol. 251)

Complaints to the PA Department of Education (PDE) –

When a dispute arises regarding enrollment of a student, the person attempting to enroll the child or the school district may bring the dispute to the attention of PDE's School Services Office. A complaint may be filed by mail, email or by phone with written follow-up. After receipt of a complaint, a PDE representative will contact the school district,

family or other involved parties to determine the facts, whether the child is entitled to enrollment in the district and to try to resolve the problem. These contacts, whenever possible, will occur within five (5) school days of receipt of the complaint.

NOTE: Check with 202 document proof.

Dallastown Area School District

Policy 201 — Admission of Students

Printed 7/9/2026

Policy Number	201
Title	Admission of Students
Adopted	4/18/2013
Revised	1/21/2021

201

Admission of Students

📅 Adopted: 4/18/2013 📅 Last Revised: 1/21/2021

Authority

The Board shall establish age requirements for the admission of beginning students which are consistent with law and regulations.[\[1\]](#)[\[2\]](#)[\[3\]](#)

Guidelines

Compulsory school age refers to the period of a child's life from the time the child enters school as a beginner, which may be no later than at the age of six (6) years, until the age of eighteen (18) or graduation from a high school, whichever occurs first.[\[4\]](#)

Kindergarten

A child is eligible for admission to kindergarten if s/he has attained the age of five (5) years of age prior to September 1st. The district does not admit any child whose age is less than the district's established admission age for kindergarten. The district may admit any child to kindergarten who has attained the age of six (6) prior to the first day of the school term with the consent of the child's parent/guardian in accordance with state law and regulations.[\[5\]](#)

First Grade

Beginners are students entering the lowest grade of the primary school above the kindergarten level. Beginners shall be admitted to the school during the first two (2) weeks of the annual school term and thereafter at the district's discretion. A beginner is eligible for admission to the first grade if s/he has attained the age of six (6) years prior to September 1. A child who is six (6) years of age shall be admitted to school at any time during the school year in accordance with state law and regulations.[\[4\]](#)[\[6\]](#)[\[7\]](#)

Per 22 PA Code, Sec. 11.15, the district may have a minimum beginner age no higher than six (6) years and no months on the first day of the school term. Also, the district's minimum age may not be less than 5 years, 7 months before September 1st.

The district is not required to admit as a beginner any child whose age is less than the district's established admission age for beginners.[\[8\]](#)

Admission of Transfers

Students transferring from another school district must present all requisite proofs of age, proof of residency, and immunizations, as well as transfers and school records from the district from which the transferring student came, and such other data as will assist the building principal or registrar in making a proper placement of the transferring student, as well as any additional matters as set forth in the Basic Education Circular, Enrollment of Students, dated January 22, 2009, and as amended from time to time.[\[1\]](#)[\[6\]](#)[\[9\]](#)[\[10\]](#)[\[11\]](#)[\[12\]](#)[\[13\]](#)

Delegation of Responsibility

The Superintendent or designee shall require that the parent/guardian of each student who registers for entrance to school shall submit proof of age, two (2) proofs of residency, and required immunizations.[\[13\]](#)[\[14\]](#)

Footnotes

[1] 24 P.S. 1301 [View source](#) [↗](#)

[2] 22 PA Code 11.12 [View source](#) [↗](#)

[3] 22 PA Code 11.41 [View source](#) [↗](#)

[4] 24 P.S. 1326 [View source](#) 

[5] 22 PA Code 11.14 [View source](#) 

[6] 24 P.S. 1304 [View source](#) 

[7] 22 PA Code 11.15 [View source](#) 

[8] 22 PA Code 11.16 [View source](#) 

[9] 24 P.S. 1302 [View source](#) 

[10] 24 P.S. 1305 [View source](#) 

[11] 24 P.S. 1306 [View source](#) 

[12] 24 P.S. 1303a [View source](#) 

[13] **Pol. 200**
Policy Reference [Open policy](#) 

[14] **Pol. 203**
Policy Reference [Open policy](#) 

Dallastown Area School District

Policy 201-AR-0 — Admission of Students

Printed 7/9/2026

Policy Number 201-AR-0
Title Admission of Students
Adopted 10/6/2016
Revised 1/21/2021

201-AR-0

Admission of Students

📅 Adopted: 10/6/2016 📅 Last Revised: 1/21/2021

When a student who meets the age requirements of Board policy is presented for admission into kindergarten or first grade, school staff will require the following documentation, as outlined in district Policy 200 Enrollment of Students and Administrative Regulations 200-AR, and 200-AR-1:

1. Proof of the student's date of birth – acceptable documentation includes one (1) of the following:

Birth Certificate	Baptismal Certificate
Duly Certified/Notarized Transcript of the Record of Baptism	Duly attested transcript of birth certificate
Duly Certified/Notarized Transcript of Birth	Valid Passport
Notarized statement from parent/guardian or relative indicating date of birth	

2. Immunization record with dates, assurance from the former school district, or, a medical office that the required immunizations have been completed or a required series has begun, with a record to be sent. Written statements are required for religious and medical exemptions.

3. Proof of residency – acceptable documentation includes one (1) from each of the following lists:

a. List A

- i. Lease Agreement or Rent Payment Receipts. (This is **required** if you are not the owner of the property. If you are not the owner of the property and cannot provide a lease, you and the owner/leaseholder will be required to complete and submit a notarized Shared Residency Affidavit.)
- ii. Current utility bill with current address (acceptable as List A item **only** if you are the property owner; cell phone bill is not valid as proof of home ownership).
- iii. Settlement Statement.
- iv. Real Estate Tax Bill.

b. List B

- i. PennDOT issued Driver's License, Photo ID or Vehicle Registration.
 - ii. Current utility bill with current address (cannot be used if chosen as proof from List A).
 - iii. Paycheck stub with employer address and employee address.
 - iv. Current voter registration.
 - v. State/Federal program enrollment, bank statement.
4. Parent Registration Statement attesting to whether the student has been or is suspended or expelled for offenses involving drugs or alcohol, weapons or violence as required by the Pennsylvania School Code.
5. Home Language Survey – All students seeking first time enrollment in a school shall be given a home language survey in accordance with requirements of the U.S. Department of Education's Office for Civil Rights. Enrollment of the student may not be delayed in order to administer the Home Language Survey.

Kindergarten and first grade students will be admitted during the first two (2) weeks of the school term. Later admissions of students less than six (6) years old must be reviewed/approved by the Superintendent or designee. Students transferring from another school and students who are six (6) years old will be admitted at any time.

A student who has been attending an approved kindergarten program in another district or state and does not meet the Board's established age requirements will be permitted to enter the district's program, upon presentation of the required documentation, provided the student is eligible to enroll in accordance with District Policy 201 Admission of Students.

Parents/Guardians will be notified of timelines for kindergarten enrollment and student screening. Kindergarten readiness screening will be conducted by district staff prior to the beginning of the school term.

The registrar will report to the Superintendent or designee the name of any student attempting to enroll in kindergarten or first grade who does not present the required documentation.

References:

Board Policy- 200, 201, 202, 203