Book	Policy Manual
Section	7000 Property
Title	Copy of MAINTENANCE
Code	po7410 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018

7410 - **MAINTENANCE**

The Board ~~of Education~~ recognizes that the capital ~~fixed~~ assets of ~~this~~ the District represent a significant investment of this community and ~~their~~ the maintenance of those assets is of ~~prime~~ concern to the Board.

The Board directs the conduct of a continuous program of inspection, maintenance, and rehabilitation for the preservation of all school buildings, ~~and~~ equipment, and District grounds. Wherever possible and feasible, maintenance shall be preventive.

The District Administrator shall develop, for implementation within budget allocations approved by the Board, a maintenance program that shall include:

A. **(x)** a regular summer program of facilities repair and conditioning;

B. **(x)** the maintenance of a critical spare parts inventory;

C. **(x)** an equipment replacement program;

D. **(x)** a long-range program of buildingfacilities refurbishment and modernization;

E. **(x)** repair or replacement of equipment or facilities for energy conservation, safety, or other environmental factors.

Disabled parking spaces and signs, in conformance with State law, shall be provided where deemed necessary.

Book	Policy Manual
Section	7000 Property
Title	Copy of SAFETY STANDARDS
Code	po7430 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018
Last Revised	November 10, 2021

7430 - **SAFETY STANDARDS**

The Board believes that the employees and students of this District, as well as visitors, are entitled to function in an environment as free from hazards as can reasonably be provided. In this regard and in accordance with law, the Board will provide reasonable and adequate protection to the lives, safety, and health of its employees, students, and visitors.

The District Administrator shall be responsible for the maintenance of standards in the facilities to prevent accidents and to minimize their consequences. ~~S/He~~ The District Administrator shall designate an employee who shall conduct periodic audits of health and safety conditions within the facilities of the District in accordance with the Federal OSHA standards adopted by the State, and take appropriate action on any violations ~~thereof~~ discovered during such audits. Reports of violations and remediation actions shall be provided to the District Administrator who shall keep the Board informed of significant issues.

In the event an inspection is made by a representative of the State and a violation is indicated on the inspection report, the District Administrator shall report the violations(s) and corective action(s) ~~results thereof~~ to the Board no later than at the meeting following the receipt of the State report.

~~T.C. 11/10/21~~

Legal	101.055, Wis. Stats.

Book	Policy Manual
Section	7000 Property
Title	Copy of SMART SENSOR AND MONITORING TECHNOLOGY
Code	po7440.02 KMK 12-26-24
Status	Proposed
Adopted	October 23, 2023

7440.02 - **SMART SENSOR AND MONITORING ~~EQUIPMENT~~ TECHNOLOGY**

In order to protect students and faculty, promote security and protect the health, welfare and safety of students, staff and visitors, the Board authorizes the use of smart sensor and electronic monitoring equipment on school property, and in school buildings and school buses. Smart sensor and monitoring technology uses devices that can sense, collect, and process a variety of environmental information. Information obtained through smart sensor devices may be used to identify intruders and persons breaking the law, Board policy, or the Student Code of Conduct (i.e., it may be used as evidence in disciplinary actions and criminal proceedings).

The monitoring of actions and behavior of individuals who come onto school property is a significant factor in maintaining order and discipline and protecting students, staff, visitors, and school and student property. Smart sensor monitoring systems serve to complement other means being employed in the District to promote and foster a safe and secure teaching and learning environment for students and staff. The Board recognizes that the use of a smart sensor monitoring system does not replace the need for the ongoing vigilance of the school staff assigned by the building principal to monitor and supervise the school building. Rather, the smart sensor monitoring system serves as an appropriate and useful tool with which to augment or support the in-person supervision provided by staff. The building principal is responsible for verifying that due diligence is observed in maintaining general campus safety and security.

The District Administrator is responsible for determining where to install and operate fixed-location smart sensor monitoring equipment in the District. The determination of where and when to use smart sensor equipment will be made in a nondiscriminatory manner. Smart sensor equipment may be placed in designated areas in school buildings (e.g., school hallways, restrooms, classrooms, locker rooms, entryways, the front office where students, employees, and visitors are permitted to freely come and go, gymnasiums, cafeterias, libraries).

Any person who takes action to block, move, or alter the location of a smart sensor shall be subject to disciplinary action.

Any information obtained from smart sensor monitoring systems may only be used to support the orderly operation of the ~~School~~ District's schools and facilities, and for law enforcement purposes, and not for any other purposes. As such, information obtained through the use of smart sensor equipment may be used as evidence in any disciplinary proceedings, administrative proceedings or criminal proceedings, subject to Board policy and ~~regulations~~ administrative guidelines.

Smart sensor technology is to be implemented in accordance with this policy and ~~the~~ any related guidelines. The Board will not accept or tolerate the improper use of smart sensor ~~equipment~~ and monitoring technology and will take appropriate action in any cases of wrongful use of ~~this policy~~ such technology.

Book	Policy Manual
Section	7000 Property
Title	Copy of FACILITY SECURITY
Code	po7440 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018
Last Revised	April 10, 2024

7440 - **FACILITY SECURITY**

Promoting the safety of students, staff, and others in the school buildings, as well as providing for the protection of the significant financial investment in the District's buildings is a critical function of the Board. Proper safety measures are to be implemented to protect those who use the buildings and to protect the buildings and equipment owned by the Board from theft and vandalism in order to maintain the optimum conditions for carrying out the educational program.

The District Administrator shall develop and supervise a program for the security of the District's students, staff, visitors, school buildings, school grounds, and school equipment in compliance with State and Federal laws as described in Policy 8420 - School Safety.

~~Every effort shall be made~~ Law enforcement shall be contacted and District officials shall fully cooperate with law enforcement's efforts to apprehend those who knowingly cause ~~serious~~ physical harm to students, staff, visitors, and Board property and to ~~require~~ request prosecution of those who bring harm to persons and/or property. The Board will seek to repair the damage or seek the payment of a fee to cover such repairs.

The Board authorizes the District Administrator to conduct searches of non-student visitors or vehicles on school property when there is a reasonable suspicion of violation of the law or school rules, and the search is reasonable in scope related to the objectives of the search and not excessively intrusive.

~~Appropriate authorities may be contacted in the case of serious offenses.~~

The District Administrator is authorized to utilize metal detectors (e.g., walk-through detectors and hand-held wands), video surveillance/electronic monitoring equipment, and other secury devices on school property in order to protect the health, welfare and safety of students, staff, visitors and Board property in school buildings or on District property.

The District Administrator shall report to the Board as soon as reasonable, any significant incident involving vandalism, theft, personal safety or other security risks and the measures being taken to address the situation.

Public Access to School Facilities

The Board expects that during regular school hours only students and school staff need to be present in the school building. The Board also acknowledges that there will be times during the instructional day that members of the public, including parents, invited guests, or other individuals will for appropriate and legitimate reasons require entry into a school facility. In such cases, the following guidelines shall be followed:

A. All exterior doors shall be locked during the instructional day, preventing entry into the building and all visitors to the school building during those times will be directed to a single entrance into the building. This entrance shall be the entrance at door #2. Visitors must identify themselves and the purpose of their visit to the school through the

intercom system. The exception would be a scheduled event that the public is invited to attend.

B. All persons other than students and building staff shall check in with the main office of the building and shall complete a visitor log. Each visitor shall be given a visitor tag that shall be worn at all times while in the building.

C. Visitors that intend to visit a classroom during the instructional day may be escorted to the classroom by either a staff member or, if age-appropriate, a student from the class. Main office staff must contact the classroom teacher to verify that the visitor is expected.

D. All visitors are expected to sign out prior to departing the building.

E. Outside of instructional times, no person other than a staff member may be in any school buildings except for attendance at a public function (such as a sporting event, practice, civic meetings or activities) or based on an approved facility use request pursuant to Policy 7510 - Use of District Facilities.

Any visitor to the school may be refused entry or asked to leave the building at any time if a Building Administrator or event supervisor determines that the visitor's presence is disruptive or is likely to become disruptive to the educational environment, including all school-sponsored events, or for other safety or security reasons. If a visitor refuses to leave upon request by a building adminstrator or event supervisor, the building administrator or event supervisor shall contact the school resource officer or local law enforcement as appropriate. No staff member should attempt to physically remove a visitor unless the visitor poses an imminent safety threat.

Failure to follow the requirements above when entering or remaining in school facilities may be subjected to a fine not exceeding $1,000 in circumstances tending to provoke a disturbance of the peace, may be fined not more than $10,000 or imprisoned not more than ninety (90) days.

Any school staff member that witnesses a visitor in the school building who is not wearing a visitor tag as required shall report the visitor's presence to the main office. In the event the main office does not have record of such visitor properly checking in, the office staff shall immediately contact an administrator or, if any administrator is not available, the school resource officer, if applicable, or appropriate law enforcement.

Parents as Visitors

The Board encourages parental involvement in the education of students in the District. For this reason, it is important to facilitate the involvement of parents in school activities and the educational process while at the same time preserving the integrity of the educational environment for all students. As a balance, the Board adopts the following requirements for parents visiting the school during the instructional day:

A. Parents should make arrangements with their child's teacher or with the building administrator in advance of visiting their child at school unless that is not possible.

B. Parents, like any other visitor, must enter the building through only the approved visitor entrance and shall check in at the school office in the same fashion as a visitor.

Parents visiting District schools shall comply with Policy 9150 - School Visitors, and other relevant policies and administrative guidelines.

Parents who ~~that~~ do not follow these guidelines or whose presence is disruptive to the educational environment may be asked to leave the building by a building administrator. Any decision to permanently expel a parent may only be made by the District Administrator due to repeated failure to follow rules causing a disruption to the educational environment or for overt threats of harm or actual physical contact with any staff or student.

Court Imposed Restrictions

In any case in which an individual is the subject of a court order restricting the individuals presence at a school building, including any restrictions on the individuals physical proximity to an individual that is a student or staff member at the school facility, the building administrator shall inform staff of the situation and if any staff member sees the individual on school premises that staff member shall immediately contact law enforcement and the main office.

Sex Offenders on School Property

Any person ~~that s~~ who is a registered sex offender under Wisconsin Law is required to notify the District Administrator of the specific date, time and place of the person's visit to any school facility and must notify the District Administrator of their status as a registered sex offender.

Parents of students enrolled in the District must notify the District Administrator of their status as a registered sex offender and that they have a child enrolled in the District. Notification must occur at the beginning of each school year or at the time the individual is required to register or whenever the child is first enrolled, whichever occurs first.

Notification requirements do not apply if the person will be on school grounds to vote in an election or to attend a non-school sponsored event occurring on the school grounds.

~~Revised 5/13/19~~
~~Revised 4/12/23~~
~~T.C. 10/23/23~~

Legal

120.13(35), Wis. Stats.

175.32(2), (3), Wis. Stat.

301.475, Wis. Stat.

State v. Vang, 2018 AP 1730 (Ct. App. 2021), pet. rev. denied.

Book	Policy Manual
Section	7000 Property
Title	Copy of STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018
Last Revised	November 11, 2020

7540.03 - **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning to incorporate the vast, diverse, and unique resources available through the Internet. The Board provides technology resources (as defined in Bylaw 0100 - Definitions) to support the educational and professional needs of its students and staff. With respect to students, District Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and Internet system do not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District technology resources by principles consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of District Technology Resources and students' personal communication devices when they are connected to the District computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity (see Policy 5136 - Personal Commmunication Devices).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

The Board may not be able to technologically limit access to services through its technology resources to only those that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures, that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or the District Administrator, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measures may not be disabled at any time that students may be using the District technology resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Board utilizes software and/or hardware to monitor online activity of students and to block/filter access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. "Harmful to minors" is a term defined by the Communications Act of 1934 (47 U.S.C. 254(h)(7)) as any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

B. 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 a lewd exhibition of the genitals;

C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

At the discretion of the Board or the District Administrator, the technology protection measure may be configured to protect against access to other material considered inappropriate for students to access. The technology protection measure may not be disabled at any time that students may be using the District technology resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The District Administrator may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measure. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measure.

The District Administrator may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Parents are advised that a determined user may be able to gain access to services and/or resources on the Internet that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents may find inappropriate, offensive, objectionable or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

B. the dangers inherent with the online disclosure of personally identifiable information;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students online;

D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

Staff members shall provide instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

Building Principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including

in chat rooms, and cyberbullying awareness and response. All users of District technology resources (and their parents if they are minors) are required confirm their agreement to abide by the terms and conditions of the policy and it's accompanying guidelines by signing the District technology use form.

Off premises use of E-Rate supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

Students will be assigned a school email account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned email account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

Students are responsible for good behavior when using District technology resources - i.e., behavior comparable to that expected of students when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its technology resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District technology resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District technology resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the District Administrator as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District technology resources.

~~Revised 4/8/20~~

Legal

H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246

47 C.F.R. 54.500

47 C.F.R. 54.501

47 C.F.R. 54.502

47 C.F.R. 54.503

47 C.F.R. 54.504

47 C.F.R. 54.505

47 C.F.R. 54.506

47 C.F.R. 54.507

47 C.F.R. 54.508

47 C.F.R. 54.509

47 C.F.R. 54.511

47 C.F.R. 54.513

47 C.F.R. 54.514

47 C.F.R. 54.515

47 C.F.R. 54.516

47 C.F.R. 54.517

47 C.F.R. 54.518

47 C.F.R. 54.519

47 C.F.R. 54.520

47 C.F.R. 54.522

47 C.F.R. 54.523

Book	Policy Manual
Section	7000 Property
Title	Copy of STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.04 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018
Last Revised	October 23, 2023

7540.04 - **STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning to incorporate the vast, diverse, and unique resources available through the Internet. The Board provides Technology and Information Resources (as defined by Bylaw 0100 - Definitions) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system do not serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy, Policy 7544, and any applicable employment contracts govern the staffs' use of the District's computers, laptops, tablets, personal communication devices (as defined by Policy 7540.02 - Web Content, Apps, and Services), when they are connected to the District computer network, Internet connection, and/or educational services/apps.

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District technology and information resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources to enrich educational activities. The instructional use of the Internet and online educational services will be guided by the Board's Policy 2521 - Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that provides a valuable education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District technology and resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such a vast quantity of information and resources brings with it, however, certain unique challenges.

The Board may not be able to technologically limit access to services through its technology resources to only those that have been authorized for the purpose of instruction, study, and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented technology protection measures, that protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the Board or District Administrator, the technology protection measures may also be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors. The technology protection measures may not be disabled at any time that students may be using the District's technology resources if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.

The District Administrator or Building Principal may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether the material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The District Administrator or Building Principal may disable the technology protection measure to enable access for bona fide research or other lawful purposes for staff or students aged seventeen (17) or older.

Staff members will participate in professional development programs in accordance with the provisions of this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social networking sites and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate technology use and online safety and security as specified above, and staff members will monitor students' online activities while at school.

Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.

The disclosure of personally identifiable information about students online is prohibited.

Building Principals are responsible for providing training so that staff users of District technology resources under the Principal's supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including chat rooms and cyberbullying awareness and response. All users of District technology resources are required to confirm their agreement by the terms and conditions of this policy and it's accompanying guidelines by signing the District technology use form. Pursuant to Policy 7540.06 - District-Issued Staff E-Mail Account, staff and Board members using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use of District-issued email accounts.

Off premises use of E-Rate supported technology must be primarily for an educational purpose that is integral, immediate, and proximate to the education of students.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the District.

With prior approval from the District Administrator or Building Principal, staff may direct students who have been issued school-assigned email accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District technology and information resources - i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of the technology and information resources that is not authorized by or conducted strictly in compliance with this policy and Policy 7544.

Staff members may only use District technology resources to access or use social media if it is done for educational or business-related purposes.

Staff members use of District technology resources to access or use social media is to be consistent with Policy 7544.

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's personal computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

General school rules for behavior and communication apply.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District technology and information resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the District Administrator and Building Principal as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District technology and information resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330 - Student Records. Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential employee information may be disciplined.

Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

~~Revised 2/12/20~~
~~Revised 11/11/20~~
~~T.C. 10/23/23~~

Legal

P.L. 106-554, Children's Internet Protection Act of 2000

47 U.S.C. 254(h, 1), Communications Act of 1934, as amended

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

18 U.S.C. 2256

18 U.S.C. 1460

18 U.S.C. 2246

20 U.S.C. 6777

20 U.S.C. 9134 (2003)

47 C.F.R. 54.500

47 C.F.R. 54.501

47 C.F.R. 54.502

47 C.F.R. 54.503

47 C.F.R. 54.504

47 C.F.R. 54.505

47 C.F.R. 54.506

47 C.F.R. 54.507

47 C.F.R. 54.508

47 C.F.R. 54.509

47 C.F.R. 54.511

47 C.F.R. 54.513

47 C.F.R. 54.514

47 C.F.R. 54.515

47 C.F.R. 54.516

47 C.F.R. 54.517

47 C.F.R. 54.518

47 C.F.R. 54.519

47 C.F.R. 54.520

47 C.F.R. 54.522

47 C.F.R. 54.523

Book	Policy Manual
Section	7000 Property
Title	Copy of ASSISTIVE TECHNOLOGY AND SERVICES
Code	po7540.05 KMK 12-26-24 TC
Status	Proposed
Adopted	July 9, 2018
Last Revised	August 14, 2024

7540.05 - **ASSISTIVE TECHNOLOGY AND SERVICES**

Students with disabilities have special challenges and may need assistive technology in order to more fully participate in their classrooms, homes, communities and workplaces. Through the use of assistive technology and services these students will have the opportunity to become more independent and self-reliant.

Each IEP team must include in ~~their~~ its deliberations consideration of whether the use of assistive technology devices and services to aid students with disabilities is appropriate for each specific student. The Board also directs that students who qualify under Section 504 of the Rehabilitation Act be provided with assistive technology devices and services when deemed necessary.

The Board also directs that students who qualify under Section 504 of the Rehabilitation Act be provided with assistive technology consistent with the student's 504 Plan.

Students having special needs but not requiring a formal IEP or 504 Plan according to law, which may include but are not limited to migrant students, homeless students, students living with poverty, and English ~~Language~~ Learners, will also be considered for assistive technology devices and/or services.

"Assistive technology device" means any item, piece of equipment, or product system, whether acquired commercially off the shelf, modified, or customized, that is used to increase, maintain, or improve functional capabilities of a child with a disability. The term does not include a medical device that is surgically implanted, or the replacement of such device.

"Assistive technology service" means any service that directly assists a child with a disability in the selection, acquisition, or use of assistive technology devices. Assistive technology services include:

A. the evaluation of needs including a functional evaluation, in the child's customary environment;

B. purchasing, leasing, or otherwise providing for the acquisition of assistive technology devices;

C. selecting, designing, fitting, customizing, adapting, applying, maintaining, repairing, or replacing of assistive technology devices;

D. coordinating and using other therapies, interventions, or services with assistive technology devices, such as those associated with existing education and rehabilitation plans and programs;

E. training or technical assistance for a child with disabilities, or where appropriate that child's family;

F. training or technical assistance for professionals (including individuals providing education and rehabilitation services), employers or other(s) who provide services to employ, or are otherwise, substantially involved in the major life functions of that child.

The Board encourages the faculty to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize assistive technology resources and assistive technology services.

Assistive technology used in conjunction with a student's Individual Education Plan (IEP) shall be used with any external communication or recording function disabled, except as provided for in the student's IEP.

The Board designates the District Administrator and the Building Principal as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to the use of assistive technology and services in the District.

Legal

Individuals with Disabilities Education Act (IDEA), as amended

20 U.S.C. 1401

Section 504 Rehabilitation Act of 1973

Assistive Technology Act (P.L. 105 394) 1998

Book	Policy Manual
Section	7000 Property
Title	Copy of DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT
Code	po7540.07 KMK 12-26-24
Status	Proposed
Adopted	July 9, 2018
Last Revised	April 13, 2022

7540.07 - **DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT**

Students assigned a school email account are required to utilize it for all school-related electronic communications, including those to staff members and individuals and/or organizations outside the District with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned email account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

This policy and any corresponding guidelines serve to establish a framework for student's proper use of e-mail as an educational tool.

Personal e-mail accounts on providers other than the District's e-mail system may be blocked at any time if concerns for network security, SPAM, or virus protection arise. Students are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

[x] Students are prohibited from using any District-issued email address, or password for the District-issued email account, for personal accounts in third-party services (e.g., Facebook, X, Instagram, Pinterest, YouTube, etc.) **(x)** without authorization from the Principal **[END OF OPTION]**.

Students shall not send or forward mass e-mails, even if educationally-related, without prior approval of their classroom teacher or the Building Principal.

Students may join list servs or other e-mail services (e.g. RSS feeds) that pertain to academic work, provided the emails received from the list servs or other e-mail services do not become excessive exceed the students' individual e-mail storage allotment. If a student is unsure whether they have adequate storage or should subscribe to a list servs or RSS feed, the student should discuss the issue with a classroom teacher, the building principal or the District's IT staff. The Building Principal is authorized to block e-mail from list servs or e-mail services if the e-mails received by the student becomes excessive megabytes.

~~Students are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages and purging e-mails once they are read and no longer needed for school.~~

Unauthorized E-mail

The Board does not authorize the use of its Technology Resources, including its computer network ("network"), to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to

send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e–mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.03 - Student Technology Acceptable Use and Safety, students using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety.

Furthermore, students using the District's e-mail system shall satisfactorily complete training **(x)**, pursuant to Policy 7540.03 - Student Technology Acceptable Use and Safety, regarding the proper use of e-mail

~~T.C. 4/13/22~~