NOTICE

SCHOOL DISTRICT OF NEW GLARUS
BOARD OF EDUCATION
POLICY, SPORTS, AND CO-CURRICULAR COMMITTEE MEETING
MONDAY, OCTOBER 23, 2017
HS CONFERENCE ROOM
6:45 PM

AGENDA

I. **CALL MEETING TO ORDER - KEITH STEFFEN**

II. **NEOLA POLICY UPDATES**

PURSUANT TO APPLICABLE LAW, NOTICE IS HEREBY GIVEN THAT A QUORUM OR A MAJORITY OF THE NEW GLARUS SCHOOL DISTRICT BOARD MEMBERS MAY ATTEND THIS MEETING. INFORMATION PRESENTED AT THIS MEETING MAY HELP FORM THE RATIONALE BEHIND FUTURE ACTIONS THAT MAY BE TAKEN BY THE NEW GLARUS SCHOOL DISTRICT BOARD.

III. **ADJOURNMENT**

POSTED :

NG HIGH SCHOOL
NG MIDDLE SCHOOL
NG ELEMENTARY SCHOOL
NG POST OFFICE
BANK OF NEW GLARUS
UB&T BANK OF NEW GLARUS
ANCHOR BANK OF NEW GLARUS

PURSUANT TO APPLICABLE LAW, NOTICE IS HEREBY GIVEN THAT A QUORUM OR A MAJORITY OF THE NEW GLARUS SCHOOL DISTRICT BOARD MEMBERS MAY ATTEND THIS MEETING.
INFORMATION PRESENTED AT THIS MEETING MAY HELP FORM THE RATIONALE BEHIND FUTURE ACTIONS THAT MAY BE TAKEN BY THE NEW GLARUS SCHOOL DISTRICT BOARD.

Book	Policy Manual
Section	6000 Finances
Title	Vol. 26, No. 2 New CROWDFUNDING
Number	po6605*
Status	Policy Committee Review

6605 - **CROWDFUNDING**

This policy applies to the use of any form of crowdfunding utilizing an online service or website-based platform for the financial benefit or gain of the District – be it a specific classroom, grade level, department, school, or curricular or extra-curricular activity. "Crowdfunding" refers to a campaign to collect typically small amounts of money from a large number of individuals to finance a project or fundraise for a specific cause. Through the use of personal networking, social media platforms, and other Internet based resources, funds are solicited or raised to support a specific campaign or project.

Crowdfunding activities aimed at raising funds for a specific classroom or school activity, including extra-curricular activity, or to obtain supplemental resources (e.g., supplies or equipment) that are not required to provide a free, appropriate, public education to any students in the classroom may be permitted, but only with the specific approval of the Superintendent.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	6000 Finances
Title	Copy of SYSTEM OF ACCOUNTING
Number	po6800*
Status	Policy Committee Review
Adopted	March 13, 2017

6800 - **SYSTEM OF ACCOUNTING**

As specified by the Department of Public Instruction, the Board of Education follows the Wisconsin Uniform Financial Accounting Requirements (WUFAR) as a listing of account classifications by which it keeps an accounting of all District funds. The Board has by resolution designated institutions to serve as depositories of all District funds and may, by resolution, designate additional or different institutions. The District's financial records shall show sources of revenue, amounts received, amounts expended, and the disposition of public property. The Business Manager shall complete an accounting of all capital assets to protect the financial investment of the District against catastrophic loss. Further, the Business Manager shall establish procedures and regulations necessary to properly account for capital assets and comply with generally accepted accounting principles (GAAP) and ensure that the District's capital assets are properly insured.

The District's system of accounting shall comply with all requirements of the Governmental Accounting Standards Board, Statement No. 54 (GASB 54). In accordance with GASB 54, the District will report its fund balances in the following categories:

A. **Nonspendable fund balance** - amounts that cannot be spent because they are either (a) not in a spendable form (which includes items that are not expected to be converted to cash – e.g., inventories or prepaid amounts) or (b) legally or contractually required to be maintained intact (e.g., the corpus of an endowment fund).

B. **Restricted fund balance** - amounts constrained to specific purposes by their providers (such as grantors, bondholders, and higher levels of government), through constitutional provisions, or by enabling legislation.

C. **Committed fund balance** - amounts constrained to specific purposes by the Board; to be reported as committed, amounts cannot be used for any other purpose unless the Board takes action to remove or change the constraint.

D. **Assigned fund balance** - amounts the Board intends to use for a specific purpose but are neither restricted nor committed; intent can be expressed by the Board or by an official or committee to which the Board delegates the authority.

E. **Unassigned fund balance** - amounts that are available for any purpose; these amounts are reported only in the general fund.

The Board authorizes its auditors and directs its administrative staff to take all steps necessary to comply with the requirements of GASB 54. All revenue and funds will be designated to one of the above categories.

The Business Manager shall maintain a proper accounting of all District funds. S/He shall ensure that expenditures are budgeted under and charged against those accounts that most accurately describe the purpose for which such monies are to be or have been spent. Wherever appropriate and practicable, salaries of individual employees, expenditures for single pieces of equipment, and the like shall be prorated under the several accounts that most accurately describe the purposes for which such monies are to be or have been spent.

The Business Manager shall receive all vouchers for payments and disbursements made to and by the Board, and preserve them for the statutorily required period.

The Business Manager shall implement procedures and practices that will determine: (1) Capitalization policies for District assets (i.e., which assets will be capitalized and depreciated over their estimated useful life versus which assets will be expensed in year of purchase); (2) Methods for calculating annual and accumulated depreciation expense for assets including estimates for asset lives, residual asset values, and depreciation methodology; and (3) Procedures for recording gain or loss on sale of capital assets and proceeds from the sale of capital assets in compliance with GAAP Reporting of estimated cash values

or replacement values to District insurance providers.

The Business Manager shall report to the Board on a monthly basis (or more often if required) the revenues and expenditures in the fund reporting categories established above. The Business Manager's statement shall show revenues and receipts from whatever source derived, the various appropriations made by the Board, the expenditures and disbursements therefrom, the purposes thereof, the balances remaining in each appropriation, and the District's assets and liabilities. At the end of the fiscal year such statement shall be a complete exhibit of the District's financial affairs and may be published and distributed with approval of the Board.

The Business Manager is responsible for filing in a timely manner, on behalf of the Board, an annual report with the Department of Public Instruction, on prescribed forms, that states the following:

A. amount of collections and receipts, and accounts due from each source

B. amount of expenditures for each purpose

C. amount of the District's debt, the purpose for which each item of such debt was created, and the provision made for the payment thereof, and

D. other information as required by the Department, along with the audit report as approved by the Board

The Board's annual financial statements shall also include information such as: (1) beginning and ending balances of capital assets; (2) beginning and ending balances of accumulated depreciation, and (3) total depreciation expense for the fiscal year.

Such reporting shall include description of significant capital asset activity during the fiscal year including: acquisitions through purchase or donation, sales or dispositions including the proceeds and gains or losses on the sale, changes in methods of calculating depreciation expense or accumulated depreciation, such as, estimates of useful life, residual values, depreciation methodology (e.g., straight line or other method).

Before implementing procedures or changing procedures, the Business Manager will review the proposed procedure with the auditor appointed by the Board to conduct the Board's financial audit. The procedures established shall comply with all statutorily required standards and generally accepted accounting procedures.

Legal 115.28(13), 115.30(1), Wis. Stats.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	7000 Property
Title	Copy of STAFF USE OF PERSONAL COMMUNICATION DEVICES
Number	po7530.02*
Status	Policy Committee Review
Adopted	March 13, 2017

7530.02 - **STAFF USE OF PERSONAL COMMUNICATION DEVICES**

Use of personal communication devices ("PCDs") has become pervasive in the workplace. For purposes of this policy, "personal communication device" includes computers, tablets (e.g., iPads and similar devices), electronic readers ("e-readers"; e.g. Kindles and similar devices), cell phones (e.g., mobile/cellular telephones, smartphones [e.g., BlackBerry, iPhone, Android devices, Windows Mobile devices, etc.], and/or other web-enabled devices of any type. Whether the PCD is Board-owned and assigned to a specific employee, or personally-owned by the employee (regardless of whether the Board pays the employee an allowance for his/her use of the device, the Board reimburses the employee on a per use basis for their business-related use of his/her PCD, or the employee receives no remuneration for his/her use of a personally-owned PCD), the employee is responsible for using the device in a safe and appropriate manner.

Safe and Appropriate Use of Personal Communication Devices, Including Cell Phones

~~Employees whose job responsibilities include regular or occasional driving and who use a PCD for business use are expected to refrain from using their device while driving. Safety must come before all other concerns. Regardless of the circumstances, including slow or stopped traffic, employees are strongly encouraged to pull off to the side of the road and safely stop the vehicle before placing or accepting a call. Reading or sending a text message, instant message or e-mail, or browsing the Internet using a PCD while driving is strictly prohibited. If acceptance of a call is unavoidable and pulling over is not an option, employees are expected to keep the call short, use hands-free options (e.g., headsets or voice activation) if available, refrain from the discussion of complicated or emotional topics, and keep their eyes on the road. Special care should be taken in situations where there is traffic, inclement weather, or the employee is driving in an unfamiliar area. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws while driving (including any laws that prohibit texting or using a cell phone or other PCD while driving).~~
~~Using a cell phone or other PCD while operating a vehicle is strongly discouraged. Employees should plan their work accordingly so that calls are placed, text messages/instant messages/e-mails read and/or sent, and/or the Internet browsed either prior to traveling or while on rest breaks. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws while driving (including any laws that prohibit texting or using a cell phone or other PCD while driving).~~

Employees are responsible for operating Board-owned vehicles and potentially hazardous equipment in a safe and prudent manner, and therefore, employees are prohibited from using PCDs while operating such vehicles or equipment. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws while driving.

Employees may not use a PCD in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated.

Duty to Maintain Confidentiality of Student Personally Identifiable Information - Public and Student Record Requirements

Employees are subject to all applicable policies and guidelines pertaining to protection of the security, integrity and availability of the data stored on their PCDs.

Cellular and wireless communications, including calls, text messages, instant messages, and e-mails sent from PCDs, may not be secure. Therefore, employees should use discretion in relaying confidential information, particularly as it relates to students.

Additionally, cellular/wireless communications, including text messages, instant messages and e-mails sent and/or received by a public employee or school official using his/her PCD may constitute public records if the content of the message concerns

District business, or an education record if the content includes personally identifiable information about a student. Cellular/wireless communications that are public records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. Cellular/wireless communications that are student records should be maintained pursuant to Policy 8330 – Students Records. Finally, cellular/wireless communications and other electronically stored information (ESI) stored on the staff member's PCD may be subject to a Litigation Hold pursuant to Policy 8315 – Information Management. Staff are required to comply with District requests to produce copies of cellular/wireless communications in their possession that are either public records or education records, or that constitute ESI that is subject to a Litigation Hold.

At the conclusion of an individual's employment (whether through resignation, nonrenewal, or termination), the employee is responsible for verifying all public records, student records and ESI subject to a Litigation Hold that are maintained on the employee's PCD are transferred to the District's custody (e.g., server, alternative storage device). The District's IT department/staff is available to assist in this process. Once all public records, student records and ESI subject to a Litigation Hold are transferred to the District's custody, the employee is required to delete the records/ESI from his/her PCD.

If a PCD is lost, stolen, hacked or otherwise subjected to unauthorized access, the employee must immediately notify the District Administrator so a determination can be made as to whether any public records, students records and/or ESI subject to a Litigation Hold has been compromised and/or lost. The District Administrator shall determine whether any security breach notification laws may have application to the situation. Appropriate notifications will be sent unless the records/information stored on the PCD was encrypted.

It is suggested that employees lock and password protect their PCDs when not in use.

Employees are responsible for making sure no third parties (including family members) have access to records and/or information, which is maintained on a PCD in their possession, that is confidential, privileged or otherwise protected by State and/or Federal law.

Privacy Issues

Except in emergency situations or as otherwise authorized by the District Administrator or as necessary to fulfill their job responsibilities, employees are prohibited from using PCDs to capture, record and/or transmit the words or sounds (i.e., audio) and/or images (i.e., pictures/video) of any student, staff member or other person in the school or while attending a school-related activity.

Using a PCD to capture, record and/or transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy and is not permitted.

PCDs, including but not limited to those with cameras, may not be activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include, but are not limited to, gymnasiums, locker rooms, shower facilities, rest/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The District Administrator and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

Personal Use of PCDs While at Work

During work hours personal communications made or received, regardless of whether on a PCD or a regular telephone or network computer, can interfere with employee productivity and distract others. Employees are expected to use discretion in using PCDs while at work for personal business. Employees are asked to limit personal communications to breaks and lunch periods, and to inform friends and family members of the Board's policy in this regard.

A. Excessive use of a PCD for personal business during work hours is considered outside the employee's scope of employment and may result in disciplinary action.

B. Employees are personally and solely responsible for the care and security of their personally-owned PCDs. The Board assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, personally- owned PCDs brought onto its property, or the unauthorized use of such devices.

Potential Disciplinary Action

Violation of this policy may result in disciplinary action up to and including termination. Use of a PCD in any manner contrary to local, State or Federal laws may also result in disciplinary action up to and including termination.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	7000 Property
Title	Copy of STUDENT EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY
Number	po7540.03*
Status	Policy Committee Review
Adopted	March 13, 2017

7540.03 - **STUDENT ~~EDUCATION~~ 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 of Education provides technology resources (as defined in Bylaw 0100) 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 ~~of Education~~ 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~~es~~ 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. ~~This policy and its related administrative guidelines and the Student Code of Conduct govern students' use of the District's computers, laptops, tablets, personal communication devices (as defined by Policy 7530.02), network, and Internet connection and online educational services ("Education Technology" or "Ed-Tech"). The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Education Technology. Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the network and Internet).~~

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).

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 encourages students to utilize Education Technology to develop the resource sharing, innovation, and communication skills and tools that are essential to both life and work. The instructional use of the Internet and online education services is guided by the Board's policy on instructional materials.~~
~~The Internet is a global information and communication network that provides a valuable opportunity to 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, the Education Technology provides 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.~~

First, the Board may not be able to technologically limit access to services through its ~~Education T~~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 ~~Education Technology~~ 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 ~~Network~~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 or Technology Director 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 or Technology Director 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.

~~The District Administrator shall prepare guidelines which address students' safety and security while using e-mail, chat rooms, instant messaging and other forms of direct electronic communications, and prohibit disclosure of personal identification information of minors and unauthorized access (e.g., "hacking") and other unlawful activities by minors online.~~
~~Education Technology is provided as a tool for education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.~~

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 the ~~Education Technology~~District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social ~~networking websites and~~ media including in chat rooms, and cyberbullying awareness and response. All ~~Internet~~ users of District technology resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

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 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 ~~and staff members~~ 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. General school rules for behavior and communication apply. The Board does not ~~sanction~~approve any use of ~~the Education Technology~~ its technology resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users ~~of the Board's Education Technology~~ are personally responsible and liable, both civilly and criminally, for uses o~~f the Ed Tech not autho~~rized District technology resources that are not authorized by this Board policy and its accompanying guidelines.

The Board designates the District Administrator and Technology Director as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of ~~the District's Education Technology~~District technology resources.

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 – 54.523

Last Modified by Jennifer Thayer on September 19, 2017

Book	Policy Manual
Section	7000 Property
Title	Copy of STAFF EDUCATION TECHNOLOGY ACCEPTABLE USE AND SAFETY
Number	po7540.04*
Status	Policy Committee Review

7540.04 **- STAFF ~~EDUCATION~~ 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 of Education provides Technology and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board ~~of Education~~ 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~~es~~ 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. ~~This policy and its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the District's computers, laptops, tablets, personal communication devices (as defined by Policy 7540.02), network and Internet connection and online educational services ("Education Technology" or "Ed-Tech"). The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the Education Technology. Users have no right or expectation to privacy when using the Ed-Tech (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity while on the network and Internet).~~

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 and its related administrative guidelines 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).

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 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 ~~Education Technology~~ 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, ~~the Education Technology~~ District technology and resources provide~~s~~ 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.

First, ~~The~~ Board may not be able to technologically limit access to services through its ~~Education Technology~~ 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 ~~Education Technology~~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 Technology Director 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 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 Technology Director 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 Education Technology 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 the ~~Education Technology~~District technology resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social ~~networking websites and~~ media, including in chat rooms and cyberbullying awareness and response. All users of District technology resources ~~Internet users~~ are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, ~~and their~~ parents and other staff members.

With prior approval from the District Administrator or Technology Director, 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 ~~the Board's Education Technology just as~~ 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.

General school rules for behavior and communication apply. ~~The Board does not sanction any use of the Education Technology that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.~~

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users ~~granted access to the Internet through the Board's Education Technology~~ are personally responsible and liable, both civilly and criminally, for uses of ~~the Ed-Tech~~District technology and information resources that are not authorized by this policy and its accompanying guidelines.

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

~~**Optional**~~

Social Media Use

An employee's personal or private use of social media, ~~such as Facebook, Twitter, MySpace, blogs, etc.,~~ 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 private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

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. 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.

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 – 54.523

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	7000 Property
Title	Copy of ELECTRONIC MAIL
Number	po7540.06*
Status	Policy Committee Review
Adopted	March 13, 2017

7540.06 - **DISTRICT-ISSUED STAFF E-MAIL ACCOUNT**~~**ELECTRONIC MAIL**~~

Staff

The Board of Education is committed to the effective use of electronic mail ("e-mail") by all District staff and Board members in the conduct of their official duties. This policy, as well as any guidelines developed pursuant to it are intended to establish a framework for the proper use of e-mail for conducting official business and communicating with colleagues, students, parents and community members~~as an official business tool.~~

When available, the District's e-mail system must be used by employees for any official District e-mail communications. Personal e- mail accounts on providers other than the District's e-mail system may be blocked at any time ~~due to~~ if concerns for network security, SPAM, or virus protection arise. ~~Furthermore,~~ District staff 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.

District staff may join list servs or other e-mail services (e.g. RSS feeds) that pertain to their responsibilities in the District, provided these list servs or other e-mail services do not exceed the staff member's e-mail storage allotment. ~~Staff members are required to keep their inbox and folders organized by regularly reviewing e-mail messages, appropriately saving e-mails that constitute a public record or student record and e-mails that are subject to a Litigation Hold, and purging all other e-mails that have been read. If the staff member is concerned that his/her e-mail storage allotment is not sufficient, s/he should contact the District's technology coordinator (IT staff).~~

Public Records

The District complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to District staff and Board members may be public records, or education records if their content includes personally identifiable information about a student. E-mails that are public records are subject to retention and disclosure, upon request, in accordance with Policy 8310 – Public Records. E-mails that are student records ~~should~~must be maintained pursuant to Policy 8330 – Student Records. Finally e-mails may constitute electronically stored information ("ESI") that may be subject to a l~~L~~itigation h~~H~~old pursuant to Policy 8315 – Information Management.

State and Federal law exempt certain documents and information within documents from disclosure, no matter what their form. Therefore, certain e-mails may be exempt from disclosure or it may be necessary to redact certain content in the e-mails before the e– mails are released pursuant to a public records request, the request of a parent or eligible student to review education records, or a duly served discovery request.

E-mails written by or sent to District staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns District business, or education records if their content includes personally identifiable information about a student. Consequently, staff shall comply with a District request to produce copies of e-mail in their possession that are either public records or education records, or that constitute ESI that is subject to a l~~L~~itigation h~~H~~old, even if such records reside on a computer owned by an individual staff member, or are accessed through an e-mail account not controlled by the District.

Retention

Pursuant to State and Federal law, e-mails that are public records or education records, and e-mails that are subject to a l~~L~~itigation h~~H~~old shall be retained.

The District maintains archives of all e-mails sent and/or received by users of the District's e-mail service. Staff members are

required to forward copies of any e-mails received in their personal e-mail account(s) not affiliated with the District server to their District e-mail account so that these records are also archived for future retrieval, if necessary.

Unauthorized E-mail

The Board does not authorize the use of its ~~proprietary computers~~ 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.

~~The District retains the right to monitor or access any District e-mail accounts at any time. Users should not expect that their communications sent or received through the District e-mail system will remain confidential and personal.~~

Authorized Use and Training

Pursuant to Policy 7540.04, 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 and safety by signing and submitting the District form.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	7000 Property
Title	Copy of Special Release - Tech Update - Phase III New DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT
Number	po7540.07*
Status	Policy Committee Review

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.

Students shall not send or forward mass e-mails, even if educationally-related, without prior approval of a staff member.

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 exceed the students' individual e-mail storage allotment. If a student is unsure whether s/he has adequate storage or should subscribe to a list servs or RSS feed, s/he should discuss the issue with his/her classroom teacher, the building principal or the District's IT staff. The Technology Director is authorized to block e-mail from list-servs or e-mail services if the e-mails received by the student becomes excessive.

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, 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 by signing and submitting Form 7540.03 F1.

Furthermore, students using the District's e-mail system shall satisfactorily complete training, regarding the proper use of e-mail.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of Vol. 26, No. 2 Renumbered/Revised NOTIFICATION OF EDUCATIONAL OPTIONS
Number	po8146*
Status	Policy Committee Review

8146~~2370~~ - **NOTIFICATION OF EDUCATIONAL OPTIONS**

The Board of Education recognizes the need to provide alternative means by which students achieve the goals of the District.

On an annual basis, a list of all educational options available to children who reside in the District, including public school, private schools participating in a parental choice program, charter schools, virtual schools, full time open enrollment, youth options, course options, and options for students enrolled in a home-based private education program, will be provided to parents.

~~An optional plan to meet the recognized educational needs of a student shall be approved by the District Administrator. The District Administrator shall prepare a plan of educational options for use in meeting special needs.~~

~~Such options shall be consistent with Chapter 118 and may include, but not be limited to, tutorial programs, independent study, correspondence courses, work-study or school work training programs, high school equivalency programs, technical college programs, summer school, early college entrance, etc.~~

~~Credit may be granted to the student upon complete evaluation of the program.~~

~~The credit shall be placed on the student's transcript. The amount of credit counting toward graduation shall comply with the graduation requirements of the State and the District.~~

~~The District Administrator shall establish administrative guidelines where each educational option is properly analyzed, planned, and implemented and complies with all applicable requirements of the State.~~

~~A list of the educational options available to students who reside in the District shall be provided to all parents on an annual basis. The list shall include public schools, private schools participating in a parental choice program, charter schools, virtual schools, full-time open enrollment, youth options, and course options. Such notice shall be published as a Class 1 Notice, pursuant to State law requirements, and posted on its website no later than January 31st each year. This notice shall include the performance category assigned to each school within the District, including charter schools and private schools participating in parental choice and shall inform parents that the full reports described in Policy 2605 are available on the website.~~

Legal	115.385(4), Wis. Stats.
	118.15, Wis. Stats.
	118.55, Wis. Stats.
	118.57 Wis. Stats.

Last Modified by Jennifer Thayer on September 20, 2017

Book	Policy Manual
Section	8000 Operations
Title	New CONTINUITY OF ORGANIZATIONAL OPERATIONS PLAN
Number	po8300*
Status	Policy Committee Review

8300 - **CONTINUITY OF ORGANIZATIONAL OPERATIONS PLAN**

The Continuity of Organizational Operations Plan (COOP) provides the District with the capability of conducting its essential operations under all threats and conditions with or without warning. Having a plan to recover from any type of disaster regardless of the severity and consequences of the emergency is critical to recovery of operations and can minimize the impact on the District's teaching and learning, personnel, facilities, technology, transportation, food service, and other functional resources.

Scope of the Continuity Plan

The primary objective of the COOP is to restore the District's critical operational functions and the learning environment as quickly as possible after a crisis or threat event has occurred. A COOP contains critical and sensitive information that is confidential and exempt from public disclosure.

Planning for the continuity of operations of a school system in the aftermath of a disaster is a complex task. The current changing threat environment and recent emergencies, including acts of nature, accidents, technological emergencies, and terrorist attacks and threats, have increased the need for viable continuity capabilities and plans that enable the District to resume and continue the essential functions in an all-hazards environment across a full spectrum of emergencies. Such conditions have increased the importance of having continuity plans in place that provide stability of essential functions across the various levels of public government and private enterprises.

The planning and development of continuity of an organizational operations plan, as well as the ongoing review and revision of such a plan, is important for the overall District and also for each school in the District.

The District-wide plan describes how the District will respond as a total organization to a given emergency and describes the centralized resources and how they will be organized to implement command and control necessary to function during the life cycle of the event. Individual school and departmental plans contain the details related to the continuity plan for those specific sites and functional areas to prepare for an event, communicate throughout the duration of an event, assess the impact of an event on essential functions in the unit, respond to the event, and detail what will be done to recover from the event.

Preparation for, response to, and recovery from a disaster affecting administrative, educational, and support functions of the District's operations requires the cooperative efforts of external organizations, in partnership with the functional areas supporting the business of the District. This includes local government agencies, law enforcement, emergency management, medical services, and vendors necessary to District operations. The COOP outlines and coordinates all efforts by the District in cooperation with other local and State agencies and businesses to restore the essential functions of the District to the larger local community post-disaster.

The Superintendent shall recommend the COOP for Board of Education review and approval; however, the COOP shall be considered a confidential document not subject to release under State public records laws and accordingly no copies shall be provided for public review during the adoption process.

The District Administrator shall conduct a periodic review of the COOP.

Legal

Last Modified by Jennifer Thayer on September 19, 2017

Book	Policy Manual
Section	8000 Operations
Title	New INFORMATION SECURITY
Number	po8305*
Status	Policy Committee Review

8305 - **INFORMATION SECURITY**

The District collects, classifies, and retains data/information from and about students, staff, vendors/contractors, and other individuals, about programs and initiatives undertaken by the school system, and about and related to the business of the District. This information may be in hard copy or digital format, and may be stored in the District or offsite with a third party provider.
Data/information collected by the District shall be classified as Confidential, Controlled, or Published. Data/information will be considered Controlled until identified otherwise.

Protecting District *Information Resources* (as defined in Bylaw 0100) is of paramount importance. Information security requires everyone's active participation to keep the District's data/information secure. This includes Board members, staff members/employees, students, parents, contractors/vendors, and visitors who use District *Technology Resources* (as defined in Bylaw 0100) and *Information Resources*.

Individuals who are granted access to data/information collected and retained by the District must follow established procedures so that the information is protected and preserved. Board members, administrators, and all District staff members, as well as contractors, vendors, and their employees, granted access to data/ information retained by the District are required to certify annually that they shall comply with the established information security protocols pertaining to District data/information. Further, all individuals granted access to Confidential Data/Information retained by the District must certify annually that they will comply with the information security protocols pertaining to Confidential Data/Information. Completing the appropriate section of the Staff Technology Acceptable Use and Safety form (Form 7540.04F1) shall provide this certification.

All Board members, staff members/employees, students, contractors/vendors, and visitors who have access to Board-owned or managed data/information must maintain the security of that data/information and the District *Technology Resources* on which it is stored.

If an individual has any questions concerning whether this Policy applies to him/her, the individual should contact the District's Technology Director or Information Technology Department/Office.

The Superintendent shall set forth internal controls necessary to provide for the collection, classification, retention, access, and security of District Data/Information.

Further, the Superintendent is authorized to develop procedures that would be implemented in the event of an unauthorized release or breach of data/information. These procedures shall comply with the District's legal requirements if such a breach of personally- identifiable information occurs.

The Superintendent shall require the participation of staff members in appropriate training related to the internal controls pertaining to the data/information that they collect, to which they have access, and for which they would be responsible for the security protocols.

Third-party contractors/vendors who require access to Confidential Data/ Information collected and retained by the District will be informed of relevant Board policies that govern access to and use of *Information Resources*, including the duty to safeguard the confidentiality of such data/information.

Failure to adhere to this Policy and its related administrative guidelines may put data/information collected and retain by the District at risk. Employees who violate this policy and/or the administrative guidelines promulgated consistent with this policy may have disciplinary consequences imposed, up to and including termination of employment, and/or referral to law enforcement. Students who violate this Policy and/or AGs will be subject to disciplinary action, up to and including expulsion, and/or referral to law enforcement. Contractors/vendors who violate this Policy and/or AGs may face termination of their business relationships with and/or legal action by the District. Parents and visitors who violate this Policy and/or AGs may be

denied access to the District's *Technology Resources*.

The Superintendent shall conduct a periodic assessment of risk related to the access to and security of the data/information collected and retained by the District, as well as the viability of the continuity of organizational operations plan developed pursuant to Policy 8300.

Legal

Last Modified by Jennifer Thayer on September 19, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of PUBLIC RECORDS
Number	po8310*
Status	Policy Committee Review
Adopted	March 13, 2017

8310 **- PUBLIC RECORDS**

The Board of Education recognizes its responsibility to maintain the public records of this District and to make such records available for inspection and reproduction.

The public records of this District include any writing prepared, owned, used, in the possession of, or retained by the District, its Board, officers, or employees to the extent such writings are within the definition of public records under applicable law. "Public records" do not include notes for the personal use of the author, medical records, documents containing genetic information, trial preparation records, confidential law enforcement investigatory records, records the release of which is prohibited by State or Federal law.

Any person may make an oral or written request for any public records of the District. The person may inspect, copy, or receive copies of the public record requested. The District shall respond as soon as practicable and without delay to the requestor providing the requested documents or informing the requestor of the District's intent to deny access providing specific explanation regarding the decision to deny access.

No public records, including, but not limited to, personnel records, personnel files, or staff directories or student records shall include the actual/confidential addresses of students, parents, or employees who are participating in the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice. Such public records and student records shall only contain the address designated by the Wisconsin Department of Justice to serve as the student's, parent's, or employee's address. (See Policy 5111 - Eligibility of Resident/Nonresident Students, Policy 8320 - Personnel Records and Policy 8330 - Student Records.)

A resident may purchase copies of the District's public records upon payment of a fee. In cases where the cost of locating and reproducing the requested record is estimated to exceed $50, the District Administrator may require advance payment of the estimated cost from the requestor prior to fulfilling the request. The District may charge fees for the actual time spent by District employees in locating the record at the applicable employee's hourly rate for salary and benefits, as well as a reproduction cost of $0.10 per page. The District may also charge the requestor for any equipment required to fill the request (such as video tapes, computer disks, etc.). If payment is required, the District will calculate the actual cost and charge the requestor. If advance payment is required, the District will either invoice the requestor for the difference between the estimate and actual cost or refund any overpayment.

No public record may be removed from the office in which it is maintained except by a Board officer or employee in the course of the performance of his/her duties.

Nothing in this policy shall be construed as preventing a Board member from inspecting in the performance of his/her official duties any record of this District, except student records and certain portions of personnel records.

Records Retention Schedule

The District will follow the Wisconsin Department of Administration's guidelines on School District record retention. The most recent edition of the guidelines is dated May, 2010. It may be accessed at the following web address: http://publicrecordsboard.wi.gov/docview.asp?docid=15892&locid=165

Legal	19.21, 19.31-39, 120.13(12), Wis. Stats.
	29 C.F.R. Part 1635
	42 U.S.C. 2000ff et seq., The Genetic Information Nondiscrimination Act

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of PERSONNEL RECORDS
Number	po8320*
Status	Policy Committee Review
Adopted	March 13, 2017

8320 - **PERSONNEL RECORDS**

Maintaining accurate personnel records is critical to effective human resource management and to the Board of Education satisfying its legal obligations. In addition, such records frequently contain confidential information that must be managed appropriately.

Accordingly, the Board has developed the following policy relating to personnel records.

District Records Officer Designation and Responsibilities

The Board designates the Human Resources Director as the District Records Officer (DRO). The DRO will maintain a personnel file, a payroll file, an I-9 file, and a medical file for each employee. The files will be maintained in separate, secure locations. Supervisors and other administrators should forward all personnel records, I-9 records, payroll records, and medical records to the DRO to ensure that they are properly filed and maintained. Supervisors and other administrators should not maintain files containing an employee's personnel records, payroll records, I-9 records, or medical records. The DRO will also ensure that the following personnel records, if applicable, are maintained in separate, secure files:

A. criminal conviction history requests and reports

B. employee assistance program records

C. employee relations complaints including, for example, discrimination complaints

D. investigative and deliberative records relating to employee relations matters

E. privileged and confidential communications including, but not limited to, attorney-client communications

Content of Personnel Record Files

The content of the files maintained by the District shall be determined by the DRO consistent with the requirements of State and Federal law and sound principles of human resource management.

Third-Party Access to Personnel Records – Confidentiality

It is the Board's policy to respect individual privacy and to maintain in confidence all information and records pertaining to employees to the extent practicable in keeping with the Board's interest. Information in an employee's personnel file, medical file, payroll file, I-9 file and all other employment-related files will not be disclosed to any third party without an employee's written consent, except to meet the legitimate business needs of the Board or as required by law (e.g. subpoena or public record request). Further, neither the Board nor any individual employed by the Board shall access an employee's personnel records except for legitimate business purposes.

Address Confidentiality Program

Employees who are verified participants in the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice shall be permitted to use their substitute assigned address for all District purposes. The Board shall only list the address designated by the Wisconsin Department of Justice to serve as the employee's address in any personnel records, personnel files, or staff directories. Further, the Board shall use the

employee's substitute assigned address for any and all communications and correspondence between the Board and the employee. The employee's actual/confidential residential address shall be maintained in a separate confidential file that is not accessible to the public or any employees without a legitimate purpose. The intentional disclosure of an employee's actual/confidential residential address is prohibited.

Access to Personnel Documents, Employee and Designated Representative

A. **Covered Documents**

Upon the written request of an employee or former employee (the "employee"), the District shall permit the employee to inspect any personnel documents which are used or which have been used in determining that employee's qualifications for employment, promotion, transfer, additional compensation, termination or other disciplinary action, and medical records. Provided, however, that the employee has no right to inspect the following:

1. records relating to the investigation of possible criminal offenses committed by that employee

2. letter of reference for that employee

3. any portion of a test document, except that the employee may see a cumulative total test score for either a section of the test document or for the entire test document

4. materials used by the District for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions, and job assignments or other comments or ratings used for the District's planning purposes

5. information of a personal nature about a person other than the employee if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy

6. records relevant to any other pending claim between the District and the employee which may be discovered in a judicial proceeding

7. medical records that the District believes would have a detrimental effect on the employee

   In this instance, the District may release the medical records to the employee's physician or through a physician designated by the employee, in which case the physician may release the medical records to the employee or to the employee's immediate family.

B. **Request and Review Procedure**

The District shall grant at least two (2) requests by an employee in a calendar year, to inspect the employee's records as provided in this policy.

The District shall provide the employee with the opportunity to inspect the employee's records within seven (7) working days after the employee makes the request for inspection. The inspection shall take place at a location reasonably near the employee's place of employment and during normal working hours. If the inspection during normal working hours would require an employee to take time off from work, the District may provide some other reasonable time for the inspection. In any case, the District may allow the inspection to take place at a time other than working hours or at a place other than where the records are maintained if that time or place would be more convenient for the employee. The records will be reviewed in the presence of the DRO or a designee.

The employee shall not make any alterations or additions to the record nor remove any material from the record. A copy of the employee's request to review personnel records shall be filed in the employee's personnel file.

C. **Designated Representative**

An employee may designate a representative to inspect the employee's personnel records. The designation shall be in writing. The District shall allow such a designated representative to inspect that employee's personnel records in the same manner as the employee is permitted to inspect them under this guideline.

D. **Copy Charges**

The District will charge employees who wish to copy or receive a copy of records a reasonable fee for providing copies, which may not exceed the actual cost or reproduction.

Personnel Record Correction

If an employee disagrees with any information contained in the personnel records, a removal or correction of that information may be mutually agreed upon by the District and the employee. If an agreement cannot be reached, the employee may submit a written statement explaining the employee's position. The District shall attach the employee's statement to the disputed portion of the personnel record. The employee's statement shall be included whenever that disputed portion of the personnel record is released to a third party as long as the disputed record is a part of the file.

Legal 103.13, Wis. Stats.

The Americans with Disabilities Act of 1990

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of UNAUTHORIZED ACQUISITION OF STAFF PERSONAL INFORMATION
Number	po8320.01*
Status	Policy Committee Review
Adopted	March 13, 2017

8320.01 - **UNAUTHORIZED ACQUISITION OF STAFF PERSONAL INFORMATION**

The District Records Officer (DRO) will maintain a personnel file, a payroll file, an I-9 file, and a medical file for each employee. The files will be maintained in paper format.

If the DRO becomes aware of the unauthorized acquisition of "Personal Information" the DRO shall make reasonable efforts to notify each affected staff member that their personal information has been accessed. "Personal Information" includes the individual's social security number, driver's license number, State identification number, the number of financial accounts or access codes, the individual's deoxyribonucleic acid profile, or the individual's unique biometric data including fingerprint, voice print, retina or iris image, or any other unique physical representation.

No such notification is required if either (a) the acquisition of data does not create a material risk of identity theft or fraud to the individual; or (b) the personal information was acquired in good faith by a District employee or agent, and was used only for lawful purposes.

The notice shall be issued within a reasonable time, not to exceed forty-five (45) days after the District learns of the acquisition of the personal information. The notice shall indicate that the District knows of the unauthorized acquisition of personal information pertaining to the staff member. The notice shall be by mail or by a method the District has previously employed to communicate with the staff member.

Required Notice for Unauthorized Acquisition of Information

If, as the result of a single incident, the District is required to notify 1,000 or more individuals, the DRO shall without unreasonable delay notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the staff members.

Upon written request from a staff member who has received a notice, the District shall identify the personal information that was acquired.

A law enforcement agency may, in order to protect an investigation or homeland security, ask the District not to provide a notice for any period of time and the District's notification process shall begin at the end of that time period.

Legal 134.98 Wis. Stats.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of STUDENT RECORDS
Number	po8330*
Status	Policy Committee Review
Adopted	March 13, 2017
Last Revised	June 26, 2017

8330 - **STUDENT RECORDS**

In order to provide appropriate educational services and programming, the Board of Education must collect, retain, and use information about individual students. Simultaneously, the Board recognizes the need to safeguard students' privacy and restrict access to students' personally identifiable information.

Except for data identified by policy as "directory data," student "personally identifiable information" includes, but is not limited to: the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.

The Board is responsible for the records of all students who attend or have attended schools in this District. Only records mandated by the State or Federal government and/or necessary and relevant to the function of the School District or specifically permitted by this Board will be compiled by Board employees.

In all cases, permitted, narrative information in student records shall be objectively-based on the personal observation or knowledge of the originator.

Student records shall be available only to students and their parents, eligible students, designated school officials who have a legitimate educational interest in the information, or to other individuals or organizations as permitted by law.

Address Confidentiality Program

Students who are verified participants in the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice shall be permitted to use their substitute assigned address for all District purposes. The Board shall refrain from including the student's actual/confidential residential address in any student records or files (including electronic records and files) or disclosing the student's actual/confidential residential address when releasing student records. The Board shall only list the address designated by the Wisconsin Department of Justice to serve as the student's address in any student records or files, including electronic records and files. Further, the Board shall use the student's substitute assigned address for any and all communications and correspondence between the Board and the parent(s) of the student (or adult student). The student's actual/confidential residential address shall be maintained in a separate confidential file that is not accessible to the public or any employees without a legitimate purpose. The intentional disclosure of a student's actual/confidential residential address is prohibited.

The Board may enter into a memorandum of understanding with a county department under State statutes (s. 46.215, 46.22 or 46.23) or a tribal organization, as defined under Federal law, that permits disclosure of information contained in student records as provided under State law in cases in which the student's parent, if the student is a minor, or the student, if the student is an adult, does not grant permission for such disclosure

The term "parents" includes legal guardians or other persons standing in loco parentis (such as a grandparent or stepparent with whom the child lives, or a person who is legally responsible for the welfare of the child). The term "eligible student" refers

to a student who is eighteen (18) years of age.

Both parents shall have equal access to student records unless stipulated otherwise by court order or law. In the case of eligible students, parents may be allowed access to the records without the student's consent, provided the student is considered a dependent under section 152 of the Internal Revenue Code, and with respect to personally identifiable information, has not informed the school, in writing, that the information may not be disclosed.

A school official is a person employed by the Board as an administrator, supervisor, teacher/instructor (including substitutes), or support staff member (including health or medical staff and law enforcement unit personnel); a person serving on the Board; a person or company with whom the Board has contracted to perform a special task (such as an attorney, auditor, or medical consultant); a contractor, consultant, volunteer or other party to whom the Board has outsourced a service otherwise performed by Board employees (e.g. a therapist); or a parent or student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his/her tasks (including volunteers).

"Legitimate educational interest" is defined as a "direct or delegated responsibility for helping the student achieve one (1) or more of the educational goals of the District" or if the record is necessary in order for the school official to perform an administrative, supervisory, or instructional task or to perform a service or benefit for the student or the student's family. The Board directs that reasonable and appropriate methods (including but not limited to physical and/or technological access controls) are utilized to control access to student records and to make certain that school officials obtain access to only those education records in which they have legitimate educational interest.

The Board authorizes the administration to:

A. forward student records, including disciplinary records with respect to suspensions and expulsions, upon request to a private or public school or school district in which a student of this District is enrolled, seeks or intends to enroll, or is instructed to enroll, on a full-time or part-time basis, upon condition that:

    1. a reasonable attempt is made to notify the student's parent or eligible student of the transfer (unless the disclosure is initiated by the parent or eligible student; or the Board's annual notification - Form 8330 F9 - includes a notice that the Board will forward education records to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll or is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer);

    2. the parent or eligible student, upon request, receives a copy of the record; and

    3. the parent or eligible student, upon request, has an opportunity for a hearing to challenge the content of the record

B. forward student records, including disciplinary records with respect to suspensions and expulsions, upon request to a juvenile detention facility in which the student has been placed, or a juvenile court that has taken jurisdiction of the student;

C. disclose student records that are pertinent to addressing a student's educational needs to a caseworker or other representative of the department of children and families, a county department under s. 46.215, 46.22, or 46.23, or a tribal organization, as defined in 25 USC 450b(L), that is legally responsible for the care and protection of the student, if the caseworker or other representative is authorized by that department, county department, or tribal organization to access the student's case plan;

D. provide "personally-identifiable" information to appropriate parties, including parents of an eligible student, whose knowledge of the information is necessary to protect the health or safety of the student or other individuals, if there is an articulable and significant threat to the health or safety of a student or other individuals, considering the totality of the circumstances;

E. report a crime committed by a child to appropriate authorities, and, with respect to reporting a crime committed by a student with a disability, to transmit copies of the student's special education and disciplinary records to the authorities for their consideration;

F. release de-identified records and information in accordance with Federal regulations;

G. disclose personally identifiable information from education records, without consent, to organizations conducting studies "for, or on behalf of" the District for purposes of developing, validating or administering predictive tests, administering

student aid programs, or improving instruction;

Information disclosed under this exception must be protected so that students and parents cannot be personally identified by anyone other than representative of the organization conducting the study, and must be destroyed when no longer needed for the study. In order to release information under this provision, the District will enter into a written agreement with the recipient organization that specifies the purpose of the study. (See Form 8330 F14.)

This written agreement must include: (1) specification of the purpose, scope, duration of the study, and the information to be disclosed; (2) a statement requiring the organization to use the personally identifiable information only to meet the purpose of the study; (3) a statement requiring the organization to prohibit personal identification of parents and students by anyone other than a representative of the organization with legitimate interests; and (4) a requirement that the organization destroy all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed.

While the disclosure of personally identifiable information without consent is allowed under this exception, it is recommended that whenever possible the administration either release de-identified information or remove the students' names and social security identification numbers to reduce the risk of unauthorized disclosure of personally identifiable information.

H. disclose personally identifiable information from education records without consent, to authorized representatives of the Federal government, as well as State and local educational authorities. The disclosed records must be used to audit or evaluate a Federal or State supported education program, or to enforce or comply with Federal requirements related to those education programs. A written agreement between the parties is required under this exception. (See Form 8330 F16)

This written agreement must include: (1) designation of the receiving entity as an authorized representative; (2) specification of the information to be disclosed; (3) specification that the purpose of the disclosure is to carry out an audit or evaluation of a government -supported educational program or to enforce or comply with the program's legal requirements; (4) a summary of the activity that includes a description of methodology and an explanation of why personally identifiable information is necessary to accomplish the activity; (5) a statement requiring the organization to destroy all personally identifiable information when it is no longer needed for the study, along with a specific time period in which the information must be destroyed; and (6) a statement of policies and procedures that will protect personally identifiable information from further disclosure or unauthorized use.

Under the audit exception, the District will use "reasonable methods" to verify that the authorized representative complies with FERPA regulations. Specifically, the District will verify, to the greatest extent practical, that the personally identifiable information is used only for the audit, evaluation or enforcement of a government-supported educational program. The District will also ascertain the legitimacy of the audit or evaluation and will only disclose the specific records that the authorized representative needs. Further, the District will require the authorized representative to use the records only for the specified purpose and not to disclose the information any further, such as for another audit or evaluation. Finally, the District will verify that the information is destroyed when no longer needed for the audit, evaluation or compliance activity.

I. request each person or party requesting access to a student's record to abide by Federal regulations and State laws concerning the disclosure of information.

The Board will comply with a legitimate request for access to a student's records within a reasonable period of time but not more than forty-five (45) days after receiving the request or within such shorter period as may be applicable to students with disabilities. Upon the request of the viewer, a record shall be reproduced, unless said record is copyrighted, or otherwise restricted, and the viewer may be charged a fee equivalent to the cost of handling and reproduction. Based upon reasonable requests, viewers of education records will receive explanation and interpretation of the records.

The Board shall maintain a record of each request for access and each disclosure of personally identifiable information. Such disclosure records will indicate the student, person viewing the record, their legitimate interest in the information, information disclosed, date of disclosure, and date parental/eligible student consent was obtained (if required).

Only "directory information" regarding a student shall be released to any person or party, other than the student or his/her parent, without the written consent of the parent, or, if the student is an eligible student, without the written consent of the student, except as provided by applicable law.

DIRECTORY INFORMATION

Each year the District Administrator shall provide public notice to students and their parents of the District's intent to make available, upon request, certain information known as "directory information." The Board designates as student "directory information":

A. a student's name;

B. photograph;

C. participation in officially-recognized activities and sports;

D. height and/or weight, if a member of an athletic team;

E. date of graduation;

F. degrees and awards received.

Parents and eligible students may refuse to allow the Board to disclose any or all of such "directory information" upon written notification to the Board within fourteen (14) days after receipt of the District Administrator's annual public notice or enrollment of the student into the District if such enrollment occurs after the annual public notice.

In accordance with Federal and State law, the Board shall release the names, addresses, and telephone listings of secondary students to a recruiting officer for any branch of the United States Armed Forces or an institution of higher education who requests such information. A secondary school student or parent of the student may request in writing that the student's name, address, and telephone listing not be released without prior consent of the parent(s)/eligible student. The recruiting officer is to sign a form indicating that "any information received by the recruiting officer shall be used solely for the purpose of informing students about military service and shall not be released to any person other than individuals within the recruiting services of the Armed Forces." The District Administrator is authorized to charge mailing fees for providing this information to a recruiting officer.

Whenever consent of the parent(s)/eligible student is required for the inspection and/or release of a student's health or education records or for the release of "directory information," either parent may provide such consent unless agreed to otherwise in writing by both parents or specifically stated by court order. If the student is under the guardianship of an institution, the District Administrator shall appoint a person who has no conflicting interest to provide such written consent.

The Board may disclose "directory information," on former students without student or parental consent, unless the parent or eligible student previously submitted a request that such information not be disclosed without their prior written consent.

The Board shall not collect or use personal information obtained from students or their parents for the purpose of marketing or for selling that information.

INSPECTION OF INFORMATION COLLECTION INSTRUMENT

The parent of a student or an eligible student has the right to inspect upon request any instrument used in the collection of personal information before the instrument is administered or distributed to a student. Personal information for this section is defined as individually identifiable information including a student or parent's first and last name, a home or other physical address (including street name and the name of the city or town), a telephone number, or a Social Security identification number. In order to review the instrument, the parent or eligible student must submit a written request to the building principal at least fourteen (14) business days before the scheduled date of the activity. The instrument will be provided to the parent or eligible student within fourteen (14) business days of the principal receiving the request.

The District Administrator shall directly notify the parent(s) of a student and eligible students, at least annually at the beginning of the school year, of the specific or approximate dates during the school year when such activities are scheduled or expected to be scheduled.

This section does not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or educational institutions, such as the following:

A. college or other postsecondary education recruitment, or military recruitment

B. book clubs, magazine, and programs providing access to low-cost literary products

C. curriculum and instructional materials used by elementary and secondary schools

D. tests and assessments used by elementary and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments

E. the sale by students of products or services to raise funds for school- related or education-related activities

F. student recognition programs

The District Administrator shall ensure that students and parents are adequately informed each year regarding their rights to:

A. inspect and review the student's education records;

B. request amendments if the parent believes the record is inaccurate, misleading, or violates the student's privacy rights;

C. consent to disclosures of personally-identifiable information contained in the student's education records, except to those disclosures allowed by the law;

D. challenge Board noncompliance with a parent's request to amend the records through a hearing;

E. file a complaint with the United States Department of Education;

F. obtain a copy of the Board's policy and administrative guidelines on student records.

The Board authorizes the use of the microfilm process or electromagnetic processes of reproduction for the recording, filing, maintaining, and preserving of records.

No liability shall attach to any member, officer, or employee of this Board as a consequence of permitting access or furnishing student records in accordance with this policy and regulations.

Any entity receiving personally identifiable information pursuant to a study, audit, evaluation or enforcement/compliance activity must comply with all FERPA regulations. Further, such an entity must enter into a written contract with the Board delineating its responsibilities in safeguarding the disclosed information. Specifically, the entity must demonstrate the existence of a sound data security plan or data stewardship program, and must also provide assurances that the personally identifiable information will not be redisclosed without prior authorization from the Board. Further, the entity conducting the study, audit, evaluation or enforcement/compliance activity is required to destroy the disclosed information once it is no longer needed or when the timeframe for the activity has ended, as specified in its written agreement with the Board.

Legal	46.23 Wis. Stats.
	46.22 Wis. Stats.
	46.215 Wis Stats.
	118.125(2)(q) Wis. Stats.
	25 USC 450b(L)
	115.298 Wis. Stats.
	118.125 Wis. Stats.
	34 C.F.R. Part 99
	20 U.S.C., Section 1232f through 1232i (FERPA)
	26 U.S.C. 152
	20 U.S.C. 1400 et seq., Individuals with Disabilities Education Improvement Act
	20 U.S.C. 7165(b)
	20 U.S.C. 7908

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of CONFIDENTIALITY
Number	po8350*
Status	Policy Committee Review
Adopted	March 13, 2017

8350 - **CONFIDENTIALITY**

State and Federal law requires that student education records be maintained as confidential. See Policy 8330. State law further exempts certain information and records from public disclosure. See Policy 8310. As such, the Board of Education is obligated to take appropriate steps to maintain certain information and records as confidential. Individuals who have access to student education records may not remove them from Board property without express permission from their building principal or supervisor. An individual authorized to remove student education records from school property is responsible for the safety and security of the records and for returning them to the Ddistrict intact. Confidential information and records may not be disclosed except as authorized by Board policy and administrative guidelines. Individuals who have access to confidential information and records while employed by the Board are reminded that their legal obligation to maintain such confidences extends beyond their term of employment in the District and they are prohibited from releasing, disclosing or otherwise disseminating confidential information or records subsequent to leaving the Board's employ.

It is further the policy of the Board of Education that when the District receives in trust from a public agency information identified to be confidential or exempt from disclosure under the Public Records Law, Common Law, Privilege Case Law, or Federal Law, the District will maintain the confidentiality of said information to prohibit its unauthorized disclosure. The District will comply with the requirements of the Safe at Home/Address Confidentiality Program administered by the Wisconsin Department of Justice. (See Policy 5111 - Eligibility of Resident/Nonresident Students, Policy 8310 - Public Records, Policy 8320 - Personnel Records and Policy 8330 - Student Records.)

The following portions of this policy apply only to identified confidential information received from a public agency.

In order to prohibit the unauthorized disclosure of information identified as confidential by the sending public agency, the Board may seek to obtain court protection by:

A. denying requests for release of such information absent subpoena or court order;

B. pursuing motions to quash or protective orders to prohibit unauthorized disclosure.

When possible, the Board will attempt to notify the sending public agency of the request for release of such information prior to complying with the request.

Legal 19.36(1), Wis. Stats.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of AUTOMATED EXTERNAL DEFIBRILLATORS (AED)
Number	po8452*
Status	Policy Committee Review
Adopted	March 13, 2017

8452 - **AUTOMATED EXTERNAL DEFIBRILLATORS (AED)**

TheBoard of Education has determined that it may enhance school safety to have an automated external defibrillator (AED) placed in building(s) within the district.

An AED is a heart monitor and defibrillator that:

A. Is capable of recognizing the presence or absence of ventricular fibrillation or rapid ventricular tachycardia and determining without intervention by an operator, whether defibrillation should be performed.

B. Charges and, at the command of the operator, delivers an electrical impulse to an individual's heart.

The AED device(s) will be located at school buildings for use by individuals with proper AED training.

~~Students in the high school will be offered instruction in cardiopulmonary resuscitation and cardiocerebral resuscitation, and will be provided instruction about automated external defibrillators.~~
In accordance with Wisconsin Statute 118.076(3)(b), students in grades seven (7) to twelve (12) will be provided instruction about automated external defibrillators (see Policy 2413 - Health Education).

Legal	146.50(8)(g), Wis. Stats.
	118.076 Wis. Stats.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of USE OF ELECTRONIC WIRELESS COMMUNICATION DEVICES BY DISTRICT EMPLOYEES WHO OPERATE BOARD-OWNED OR OPERATED VEHICLES
Number	po8605*
Status	Policy Committee Review
Adopted	March 13, 2017
Last Revised	June 26, 2017

8605 - **USE OF ELECTRONIC WIRELESS COMMUNICATION DEVICES BY DISTRICT EMPLOYEES WHO OPERATE BOARD-OWNED OR OPERATED VEHICLES**

Personal communication devices ("PCDs"), including PCDs equipped with ear pieces, ear buds, headsets, and/or Bluetooth, shall not be used for sending or receiving text messages, or sending or reading e-mails or any other data, anytime the operator is actively driving a District school bus or other Board-owned vehicle during the course of employment, with or without students on board. No driver may use a handheld mobile telephone anytime, except for direction navigation purposes, while operating a Board-owned vehicle ~~on a highway~~, including any time where the vehicle is in operation even if temporarily stopped due to traffic or traffic control situation, except to communicate with law enforcement or other emergency services if necessary.

For purposes of this policy, electronic PCDs include, but are not limited to, cellular and wireless telephones, pagers/beepers, personal digital assistants (PDAs), Blackberries/Smartphones, any text-messaging device, and other WI-FI-enabled or broadband access devices, including computers, but does not include Citizens Band Radio or other two-way device which is installed in the vehicle and communicates directly with District transportation officials and other District vehicles only..

The mobile radio installed on all District school buses will be the primary communication system for District school bus operators. If the mobile bus radio fails, and the school bus operator's responsibility for the safety and health of the students being transported makes it necessary for the school bus driver to use a PCD while performing bus-operating duties, the school bus operator will depart the roadway, stop the bus in a safe area, and then use the PCD. Before using the PCD to send or receive a text message, the school bus or school vehicle operator must move the vehicle outside all lanes of travel and ensure that the vehicle is in a stationary position by placing the vehicle's transmission in park, or turning off the vehicle's engine, and setting the emergency brake.

Safety is always the priority while driving a school bus or other vehicle in the course of employment. Any deviation to the above policy will result in disciplinary action up to and including termination.

Legal	49 C.F.R. 392.80
	49 C.F.R. 392.82

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	8000 Operations
Title	Copy of RELIGIOUS/PATRIOTIC CEREMONIES AND OBSERVANCES
Number	po8800*
Status	Policy Committee Review
Adopted	March 13, 2017

8800 - **RELIGIOUS/PATRIOTIC CEREMONIES AND OBSERVANCES**

Decisions of the United States Supreme Court have made it clear that it is not the province of a public school to advance or inhibit religious beliefs or practices. Under the First and Fourteenth Amendments to the Constitution, this remains the inviolate province of the individual and the church of his/her choice. The rights of any minority, no matter how small, must be protected. No matter how well intended, either official or unofficial sponsorship of religiously-oriented activities by the school are offensive to some and tend to supplant activities which should be the exclusive province of individual religious groups, churches, private organizations, or the family.

District staff members shall not use prayer, religious readings, or religious symbols as a devotional exercise or in an act of worship or celebration.

~~The District shall not function as a disseminating agent for any person or outside agency for any religious or anti-religious document, book, or article.~~ Distribution of any outside organization's materials, including a request by any person wishing to facilitate dissemination of materials on District property may make a request in accordance with Policy 7510 Policy 9700 - Relations with Special Interest Groups and AG 9700A – Distribution of Materials to Students.

The Board acknowledges that it is prohibited from adopting any policy or rule respecting or promoting an establishment of religion or prohibiting any student from the free, individual, and voluntary exercise or expression of the student's religious beliefs. However, such exercise or expression may be limited to lunch periods or other non-instructional time periods when students are free to associate.

Observance of religious holidays through devotional exercises or acts of worship is also prohibited. Acknowledgement of, explanation of, and teaching about religious holidays of various religions is encouraged. Celebration activities involving nonreligious decorations and use of secular works are permitted, but it is the responsibility of all faculty members to ensure that such activities are strictly voluntary, do not place an atmosphere of social compulsion or ostracism on minority groups or individuals, and do not interfere with the regular school program.

The flag of the United States shall be raised above each school and/or at other appropriate places during all school sessions, weather permitting.

Professional staff members are authorized to lead students in the Pledge of Allegiance or the National Anthem at an appropriate time each school day. No student may be compelled against the student's objections or those of the student's parents to recite the pledge or sing the national anthem.

Every school in the District shall offer the Pledge of Allegiance or the National Anthem each school day in grades 1 through 12.

Legal	118.06(2), Wis. Stats.
	20 U.S.C. 4071 et seq.

Last Modified by Jennifer Thayer on October 12, 2017

Book	Policy Manual
Section	9000 Relations
Title	Copy of RELATIONS WITH NON-SCHOOL AFFILIATED GROUPS
Number	po9700*
Status	Policy Committee Review
Adopted	March 13, 2017

9700 - **RELATIONS WITH NON-SCHOOL AFFILIATED GROUPS**

It is the policy of the Board of Education that students, staff members, and District facilities not be used for advertising or promoting the interests of any nonschool related agency or organization, public or private, without the approval of the District Administrator or its delegated representative; and any such approval, granted for whatever cause or group, shall not be construed as an endorsement of said cause or group by this Board.

School District Referendum Advocacy

This policy applies expressly to any outside organization's advocacy concerning School District referenda. Any such organization, whether advocating in favor of or in opposition to a referendum question must clearly identify themselves as independent of the School District and may not, under any circumstances, use School District logos, mascots, slogans or other such items that are protected by or regularly used and identified with the District. School District officials may not advocate for a position on a referendum in any manner in which such advocacy is in the individual's capacity as a School District official or may reasonably be perceived as such. School District officials may always provide factual information concerning any referendum question.

A. **Materials or Activities**

All materials or activities proposed by outside organizations for student or staff use or participation shall be reviewed by the principal on the basis of the proposed activities or materials educational contribution to part or all of the school program, and benefit to students. No such approval shall have the primary purpose of advancing the name, product, or special interest of the proposing group.

1. The Board shall permit the use of educational materials, programs, and equipment which contains commercial messages providing the content of such messages and the manner of presentation has been approved by the District Administrator.

2. Outside speakers representing commercial organizations will be welcome only when the commercial aspect is limited to naming the organization represented and the subject matter advances the educational interests of the District's students.

B. **Contests/Exhibits**

The Board recognizes that contests, exhibits, and the like may benefit individual students or the District as a whole, but participation in such special activities may not:

1. have the primary effect of advancing a special product, group, or company;

2. make unreasonable demands upon the time and energies of staff or students or upon the resources of the District;

3. interrupt the regular school program;

4. involve any direct cost to the District;

C. **Distribution/Posting of Literature**

1. Non-school affiliated organizations may distribute or post literature on District property either during or after school hours only with advance permission of the principal.

2. Staff or students may be permitted to distribute literature regarding or on behalf of non-school sponsored organizations or activities, in such a manner as described in this policy and in a manner that does not disrupt or interfere with educational activities and is not done in a manner that conveys the message of endorsement or approval of the school or District of the group or message.

   Any outside organization or staff member representing an outside organization desiring to solicit funds on school property must receive permission to do so from the District Administrator.

   Decisions regarding the request to solicit funds shall not be based on the purpose or function of the group soliciting funds, unless the purpose of the organization is inappropriate for the age group of students, promotes activity that is unhealthy or unlawful, or is otherwise inconsistent with the pedagogical interests of the school.

D. **Prizes/Scholarships/Other Awards**

The Board is appreciative of the generosity of organizations which offer scholarships, prizes, or other awards to deserving students in this District.

In the administration of scholarships, prizes, or other awards, the District shall not unlawfully discriminate on the basis of sex, race, color, religion, national origin, ancestry, creed, pregnancy, marital or parental status, sexual orientation, or physical, mental, emotional, or learning disability.

Administration of scholarship or award programs appropriately designated under this policy to benefit individuals in a particular group that has not traditionally been represented does not violate this policy.

It will be the District's practice to provide all outside agencies and organizations notification of the nondiscrimination policy in awarding prizes, scholarships, or other aids, benefits, or services.

The District may administer or assist in the administration of scholarships, fellowships, or other forms of financial assistance established by a domestic or foreign will, trust, bequest, or similar legal instrument that requires the award to go to a student of a particular sex, race, color, national origin, or with a particular disability. Such restricted awards must not lead to discrimination in access to the total amount of prizes, scholarships, or other awards available.

In accepting the offer of such scholarships or prizes, the Board directs that these guidelines be observed:

No information either academic or personal shall be released from the student's record for the purpose of selecting a scholarship or prize winner without the permission of the student who is eighteen (18), or the parents of a student who is younger in accordance with the Board's policy on student records.

E.

F. The District will periodically review their procedures for awarding scholarships, prizes, and other awards. This review will require that the District's procedure does not discriminate on the basis of sex, race, color, national origin, or disability in the overall effect of the scholarships, prizes, and other awards given to students.

G.

H. Crowdfunding activities aimed at raising funds for a specific classroom or school activity, including extra-curricular activity, or to obtain supplemental resources (e.g., supplies or equipment) that are not required to provide a free, appropriate, public education to any students in the classroom may be permitted, but only with the specific approval of the District Administrator.

I.

J. **Surveys and Questionnaires**

Distribution of Surveys and Questionnaires to Students is governed by Policy 2416 - Surveys, Analyses, Evaluation.

Legal 118.125, Wis. Stats.

Last Modified by Jennifer Thayer on October 12, 2017