MSDLT Data Privacy and Security Policies

Book

Section 5000 Students

Title PERSONAL COMMUNICATION DEVICES

Code po5136

Status Active

Adopted November 16, 2015

Last Revised May 14, 2018

5136 - **PERSONAL COMMUNICATION DEVICES**

"Personal communication devices" (PCDs) as used in this policy are defined in Bylaw 0100.

Students may use PCDs before and after school, during their lunch break, in between classes as long as they do not create a distraction, disruption or otherwise interfere with the educational environment, during after school activities (e.g., extracurricular activities), or at school-related functions. Use of PCDs, except those approved by a teacher or administrator, at any other time is prohibited, and they must be powered completely off (i.e., not just placed into vibrate or silent mode) and stored out of sight.

Students may not use PCDs on school property or at a school-sponsored activity to access and/or view Internet websites that are otherwise blocked to students at school.

Students may use PCDs while riding to and from school on a school bus or other Board-provided vehicles or on a school bus or Board-provided vehicle during school-sponsored activities, at the discretion of the bus driver, classroom teacher, or sponsor/advisor/coach. Distracting behavior that creates an unsafe environment will not be tolerated.

Except as authorized by a teacher, administrator or IEP team/case conference committee ("CCC"), students are prohibited from using PCDs during the school day, including while off-campus on a field trip, 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. 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. Students who violate this provision and/or use a PCD to violate the privacy rights of another person may have their PCD confiscated. If the violation involves potentially illegal activity, the confiscated-PCD may be turned over to law enforcement.

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, classrooms, except as authorized by a teacher, administrator or IEP team/CCC, 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 Superintendent and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

Students shall have no expectation of confidentiality with respect to their use of PCDs on school premises/property.

Students may not use a PCD in any way that reasonably might create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated. See Policy 5517.01 – Bullying and Other Forms of Aggressive Behavior. In particular, students are prohibited from using PCDs to: (1) transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, color, national origin, sex (including sexual orientation/transgender identity), disability, age, religion, ancestry, or political beliefs; and (2) engage in "sexting" - i.e., sending, receiving, sharing, viewing, or possessing pictures, text messages, e-mails or other materials of a sexual nature in electronic or any other form. Violation of these prohibitions shall result in disciplinary action. Furthermore, such actions will be reported to local law enforcement and child protection services as required by law.

Students also are prohibited from using a PCD to capture, record, and/or transmit test information or any other information in a manner constituting fraud, theft, cheating, or academic dishonesty. Likewise, students are prohibited from using PCDs to receive such information.

Possession of a PCD by a student at school during school hours and/or during extra-curricular activities is a privilege that may be forfeited by any student who fails to abide by the terms of this policy, or otherwise abuses this privilege.

Violations of this policy may result in disciplinary action and/or confiscation of the PCD. The building principal also will refer the matter to law enforcement or child protection services if the violation involves an illegal activity (e.g., child pornography, sexting). Discipline will

be imposed on an escalating scale ranging from a warning to an expulsion based on the number of previous violations and/or the nature of or circumstances surrounding a particular violation. If the PCD is confiscated, it will be released/returned to the student's parent/guardian after the student complies with any other disciplinary consequences that are imposed unless the violation involves potentially illegal activity, in which case the PCD may be turned over to law enforcement. A confiscated device will be marked in a removable manner with the student's name and held in a secure location in the building's central office until it is retrieved by the parent/guardian or turned over to law enforcement. School officials will not search or otherwise tamper with PCDs in Corporation custody unless they reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules. Any search will be conducted in accordance with Policy 5771 – Search and Seizure. If multiple offenses occur, a student may lose his/her privilege to bring a PCD to school for a designated length of time or on a permanent basis.

A person who discovers a student using a PCD in violation of this policy is required to report the violation to the building principal.

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

Book

Section 5000 Students

Title TECHNOLOGY RESOURCES AND OTHER ELECTRONIC EQUIPMENT

Code po5136.01

Status Active

Adopted May 14, 2018

5136.01 - **TECHNOLOGY RESOURCES AND OTHER ELECTRONIC EQUIPMENT**

While in some instances the possession and use of Technology Resources (as defined in Bylaw 0100) and other electronic equipment or devices by a student at school may be appropriate, the possession and use of such Technology Resources and other equipment or devices by students at school also may have the effect of distracting, disrupting and/or intimidating others in the school environment and leading to opportunities for academic dishonesty and other disruptions of the educational process.

Students may use the following Technology Resources and other electronic equipment/devices during instructional time for an educational or instructional purpose (e.g. taking notes, recording a class lecture, writing papers) with the teacher's permission and supervision and may use these Technology Resources and other electronic equipment during non-instructional time, provided such use is consistent with Policy 7540.03 Student Acceptable Use and Safety:

A. cameras (photographic and/or video)

B. laptops

C. tablets (e.g., iPad-like devices)

D. smartphones

E. e-readers (e.g., Kindle-like devices)

F. personal digital assistants (PDAs)

G. portable CD/MP3 players with headphones

Students may use the following Technology Resources and other electronic equipment/devices while riding to and from school on a school bus or other vehicle provided by the Board or on a school bus or Board-provided vehicle during school-sponsored activities if approved by the student’s IEP team/CCC or at the discretion of the bus driver, classroom teacher, sponsor/advisor/coach, building principal:

A. cameras (photographic and/or video)

B. laptops

C. tablets (e.g., iPad-like devices)

D. smartphones

E. e-readers (e.g., Kindle-like devices)

F. personal digital assistants (PDAs)

G. portable CD/MP3 players with headphones

Distracting behavior that creates an unsafe environment will not be tolerated.

The preceding prohibitions do not apply to Corporation-owned and issued laptops, tablets, e-readers, PDAs, or authorized assistive technology devices.

Students are prohibited from using Technology Resources and other electronic equipment or devices in a manner that may be physically harmful to another person (e.g., shining a laser in the eyes of another student). Further, at no time may any

Technology Resources or other electronic equipment/device be utilized by a student in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed, or intimidated. See Policy 5517.01 – Bullying and Other Forms of Aggressive Behavior. In particular, students are prohibited from using Technology Resources, a camera, or other electronic equipment/device to: (1) transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex (including transgender identity, sexual orientation, and gender identity), age, disability, religion, or political beliefs; and (2) send, share, view or possess pictures, text messages, e-mails or other materials of a sexual nature (i.e., sexting) in electronic or any other form. Violation of these prohibitions shall result in disciplinary action.

Furthermore, such actions will be reported to local law enforcement and child protection services as required by law.

Students are prohibited from using Technology Resources and other electronic equipment/devices to capture, record or transmit test information or any other information in a manner constituting fraud, theft, or academic dishonesty. Similarly, students are prohibited from using Technology Resources and other electronic equipment and devices to capture, record or transmit the words (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, without express prior notice and explicit consent for the capture and/or recording of such words or images. Using Technology Resources or other electronic equipment/devices to capture, record or transmit audio and/or pictures/video of an individual without his/her consent is considered an invasion of privacy and is not permitted, unless authorized by the building principal. Technology Resources and other electronic equipment/devices are expressly banned from and may not be possessed, 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 locker rooms, shower facilities, restrooms, classrooms, except as approved by the student's IEP team/CCC, and any other areas where students or others may change
clothes or be in any stage or degree of disrobing or changing clothes. The building principal has authority to make determinations as to other specific locations and situations where possession of a camera or other electronic equipment/device is absolutely prohibited.

Unauthorized Technology Resources and other electronic equipment and devices may be confiscated from the student by school personnel and disciplinary action taken.

Any Technology Resources or other electronic equipment/device confiscated by Corporation staff will be marked in a removable manner with the student's name and held in a secure location in the building's central office until it is retrieved by the parent/guardian. Technology Resources or other electronic equipment/devices in Corporation custody will not be searched or otherwise tampered with unless school officials reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules (e.g., a student is observed using a camera in a prohibited area). Any search will be conducted in accordance with Policy 5771 – Search and Seizure.

Students are personally and solely responsible for the care and security of any Technology Resources and other electronic equipment or devices they bring to school. The Board assumes no responsibility for theft, loss, damage, or vandalism to electronic equipment and devices brought onto its property, or the unauthorized use of such devices.

Book

Section	7000 Property
Title	CORPORATION-OWNED PERSONAL COMMUNICATION DEVICES
Code	po7530.01
Status	Active
Adopted	November 16, 2015

7530.01 - **CORPORATION-OWNED PERSONAL COMMUNICATION DEVICES**

The School Board will provide personal communication devices ("PCDs") to employees who by the nature of their job have a routine and continuing business need for the use of such devices for official Board business. For purposes of this policy, "personal communication device" includes computers, tablets (e.g., iPads and similar devices), electronic readers and/or other web-enabled devices of any type. PCDs are provided as tools to conduct Board business and to enhance business efficiencies. Corporation-owned cell phones are not a personal benefit and shall not be a primary mode of communication, unless they are the most cost-effective means to conduct Board business.

The Superintendent shall designate those staff members who will be issued a Corporation-owned cell phone and provided with a cellular telephone and/or wireless Internet/data service plan.

The Superintendent or his/her designee is responsible for verifying:

A. the need for each Corporation-owned cell phone and related service plan is clearly justified for Board business purposes;

B. a Corporation-owned cell phone is returned and the corresponding cellular telephone and/or wireless Internet/data service plan is terminated when it is no longer justified by business requirements, the employee leaves the Board's employment, and/or when the employee has demonstrated a disregard for the limitation of this policy.

The Superintendent shall secure the most economical and responsible service available.

An annual review of the service plans available shall be made to determine if the Corporation's plans are the most economical and responsible available.

Possessing a Corporation-owned cell phone and/or other PCD is a privilege and all employees are expected to use them appropriately and responsibly.

In order to continue to be eligible to receive a Corporation-owned cell phone, staff members are required to answer all calls on his/her Corporation-owned cell phone and promptly respond to any messages.

In order to continue to receive a Corporation-owned cell phone and/or other PCD, non-exempt employees are required during his/her regular work hours to answer all calls on his/her cell phone and promptly respond to any messages. Non-exempt employees are not permitted to work remotely via their Corporation-owned PCD outside regular work hours without prior authorization from their supervisor. In other words, unless they are directed to provide an immediate response, all emails/texts/calls should be responded to only during regular work hours. Non-exempt employees must maintain a written record of all time spent preparing and/or responding to e-mails/texts and placing and/or answering calls outside regular work hours.

Safe and Appropriate Use of Corporation-owned PCDs, Including Cell Phones

Employee safety is a priority of the Board, and responsible use of Corporation-owned PCDs, including cell phones, requires safe use. See Policy 7530.02 - Staff Use of Personal Communication Devices.

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 Corporation-owned PCDs. See Policy 7530.02 - Staff Use of Personal Communication Devices.

When the Board intends to dispose of, or otherwise stop using, a Corporation-owned PCD on which an employee has maintained public records, student records and/or ESI that is subject to a Litigation Hold, the Corporation’s IT department/staff shall verify such records are properly transferred to an alternative storage device, before disposing of, or otherwise ceasing to use, the PCD. The IT

department/staff is responsible for securely deleting such records/ESI before disposing of, or ceasing to use, the Corporation-owned PCD. The IT department/staff is responsible for maintaining documentation concerning the actions it takes to comply with this requirement.

Employee's Responsibilities

Employees are responsible for the safekeeping, care and custody of the Corporation-owned PCDs assigned to them. Further, employees may be held financially responsible for the cost of misuse, intentional damage or reckless loss of the Corporationowned PCDs provided to them.

Reasonable precautions should be taken to prevent theft, loss or damage to, or misuse or unauthorized use/access to, Corporation-owned PCDs. Upon resignation or termination of employment, or at any time upon request, an employee may be asked to produce the Corporation-owned PCD issued to him/her for return or inspection. Employees unable to present the device might be expected to bear the cost of a replacement. Employees who separate from employment with outstanding debts for equipment loss or unauthorized charges will be considered to have left employment on unsatisfactory terms and may be subject to legal action for recovery of the loss.

Employees provided with a PCD understand that the PCD is owned by the Board.

The Board reserves the right to audit all Corporation-owned cell phones, which will include, but not be limited to, a review of the detailed monthly statement upon submission after the requisite review by the employee. The detailed monthly service statements for all Corporation-owned cell phones, as well as invoices and payment documents related to these accounts, are public records and, as such, may be subject to disclosure and review.

Potential Disciplinary Action/Cancellation of Corporation-owned PCD

Violation of this policy may constitute just cause for disciplinary action up to and including termination. Use of the Corporationowned PCD in any manner contrary to local, State or Federal laws will constitute misuse, and will result in the Board canceling the employee's privilege to use the PCD and requiring the employee to immediately return the device.

Reimbursement for Business Calls on Personally-Owned Cell Phone

If a Board employee's job duties do not include frequent need for a cell phone, the employee is not eligible to receive a Boardprovided cell phone. Such employees, however, may request reimbursement for the actual extra expenses of business-related calls that are made/received on their personally-owned cell phone. Reimbursement for per-minute "air time" charges is limited to the total overage charge shown on the invoice; expenses for minutes included in the employee's personal plan will not be reimbursed. The employee should make personal payment to the provider, and then submit a request for reimbursement, which details the date/time of the call, to whom the call was placed or from whom the call was received, and a brief description of the purpose of the call. A copy of the employee's cellular telephone service bill must be attached to the request for reimbursement (the employee may redact any personal calls from the bill prior to submitting it). Business calls made on school property should be made from traditional land-line phones, when readily accessible, and therefore will not be reimbursed if made on a personally-owned cell phone.

Book

Section

Title TECHNOLOGY

Code po7540

Status Active

Adopted November 16, 2015

Last Revised May 22, 2017

7540 - **TECHNOLOGY**

The Board is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of Corporation operations.

Students' use of Corporation Technology Resources (see definition in Bylaw 0100) is a privilege, not a right. As a prerequisite, students and their parents must sign and submit a *Student Network and Internet Acceptable Use and Safety* form annually. (See also, Policy 7540.03)

The Superintendent shall develop, recommend for approval by the Board, and implement a written Corporation Technology Plan (CTP). One of the primary purposes of the CTP is to evaluate new and emerging technologies and how they will play a role in student achievement and success and/or efficient and effective Corporation operations. The Board will financially support, as the budget permits, the CTP, including recommendations to provide new and developing technology for students and staff.

The CTP shall set forth procedures for the proper acquisition of technology. The CTP shall also provide guidance to staff and students about making safe, appropriate and ethical use of Corporation Technology Resources, as well as inform both staff and students about disciplinary actions that will be taken if its Technology Resources are abused in any way or used in an inappropriate, illegal, or unethical manner. See Policy 7540.03 and AG 7540.03 – Student Technology Acceptable Use and Safety, and Policy 7540.04 and AG 7540.04 – Staff Technology Acceptable Use and Safety.

The Superintendent, in conjunction with the Chief Technology Officer, shall review the CTP and recommend the approval of any changes, amendments, or revisions to the Board annually.

This policy, along with the Student and Staff Technology Acceptable Use and Safety policies, and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 5136 and Policy 7530.02). Users have no right or expectation of privacy when using Corporation 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 Corporation's computer network and/or Internet connection).

Further safeguards shall be established so that the Board's investment in both hardware and software achieves the benefits of technology and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media to interact with others online; interacting with other individuals in chat rooms or on blogs; and, recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Corporation policy, and learning appropriate responses if they experience cyberbullying.

For purposes of this policy, social media is defined as Internet-based applications that facilitate communication (e.g., interactive/two-way conversation/dialogue) and networking between individuals or groups. Social media is "essentially a category of online media where people are talking, participating, sharing, networking, and bookmarking online. Most social media services encourage discussion, feedback, voting, comments, and sharing of information from all interested parties." [Quote from Ron Jones of Search Engine Watch] Social media provides a way for people to stay "connected or linked to other sites, resources, and people." Examples include Facebook, Twitter, Instagram, webmail, text messaging, chat, blogs, and instant messaging (IM). Social media does not include sending or receiving e-mail through the use of Corporation-issued e-mail accounts.

The Board prohibits students from using Corporation Technology Resources to access and/or use social media.

Staff may use social media for business-related purposes. Authorized staff may use Corporation Technology Resources to access and use social media to increase awareness of Corporation programs and activities, as well as to promote achievements of staff and students, provided the Superintendent approves, in advance, such access and use. Use of social media for business-related purposes is subject to Indiana's public records laws and staff members are responsible for archiving their social media and complying with the Corporation's record retention schedule. See Policy 8310 – Public Records, AG 8310A – Public Records, and AG 8310D – Records Retention and Disposal.

Staff must comply with Policy 7540.04 and Policy 7530.02 when using Corporation Technology Resources to access and/or use social media.

Book

Section 7000 Property

Title TECHNOLOGY PRIVACY

Code po7540.01

Status Active

Adopted May 22, 2017

7540.01 - **TECHNOLOGY PRIVACY**

The Board recognizes its staff members' right to privacy in their personal lives. This policy serves to inform staff members of the Corporation's position with respect to staff-member privacy in the educational and workplace setting and to protect the Corporation's interests.

All Corporation Technology Resources (as defined in Bylaw 0100) are the Corporation's property and are to be used primarily for business purposes. The Corporation retains the right to access and review all Information Resources (as defined in Bylaw 0100), including, but not limited to electronic and voice mail, computer files, data bases, and any other electronic transmissions contained in or used in conjunction with the Corporation's computer system/network, telephone system, electronic mail system, and voice mail system. Staff members should have no expectation that any personal information/data maintained, stored, or transmitted on or through such systems is confidential or private.

Review of such information may be done by the Corporation with or without the staff member's knowledge. The use of passwords does not guarantee confidentiality, and the Corporation retains the right to access information in spite of a password. All passwords or security codes must be registered with the Corporation. A staff member's refusal to permit such access may be grounds for discipline up to and including discharge.

Corporation Technology Resources are to be used for business and educational purposes. Personal messages via Corporation Technology Resources should be limited in accordance with the Superintendent's guidelines. Staff members are encouraged to keep their personal records and personal business at home.

Because Corporation Technology Resources are to be used primarily for business and educational purposes, staff members are prohibited from sending offensive, discriminatory, or harassing computer, electronic, or voice mail messages.

Corporation Technology Resources must be used properly. Review of computer files, electronic mail, and voice mail will only be done in the ordinary course of business and will be motivated by a legitimate business reason. If a staff member's personal information is discovered, the contents of such discovery will not be reviewed by the Corporation, except to the extent necessary to determine if the Corporation's interests have been compromised. Any information discovered will be limited to those who have a specific need to know that information.

The administrators and supervisory staff members authorized by the Superintendent have the authority to search and access information electronically.

All Corporation Technology Resources and Information Resources are the property of the Corporation. Staff members shall not copy, delete, or remove any information/data contained on Corporation Technology Resources without the express permission of the Superintendent, or communicate any such information to unauthorized individuals. In addition, staff members may not copy software on to any Corporation Technology Resources and may not bring software from outside sources for use on Corporation Technology Resources without the prior approval of the Chief Technology Officer. Such pre-approval shall include a review of any copyright infringements or virus problems associated with such outside software.

Book	Policy Manual
Section	7000 Property
Title	WEB ACCESSIBILITY, CONTENT, APPS AND SERVICES
Code	po7540.02
Status	Active
Adopted	November 16, 2015
Last Revised	September 24, 2020

7540.02 - WEB ACCESSIBILITY, CONTENT, APPS AND SERVICES

Creating Content for Web Pages/Sites, Apps and Services

The Board authorizes staff members and students to create content for web pages/site(s), and apps and services (see Bylaw 0100 - Definitions) that will be hosted by the School Corporation on its servers or Corporation-affiliated servers and published on the Internet.

The content of web pages/site(s), and apps and services must comply with State and Federal law, e.g., copyright laws, Children's Internet Protection Act (CIPA), Section 504 of the Rehabilitation Act of 1973 (Section 504), Americans with Disabilities Act (ADA), and Children's Online Privacy Protection Act (COPPA), and reflect the professional image/brand of the Corporation, its employees, and students. Content of web pages/site(s), and apps and services must be consistent with the Board's Mission Statement and staff-created content for web pages/site(s), and apps and services is subject to prior review and approval of the Superintendent before being published on the Internet and/or utilized with students.

The creation of web content, for web pages/site(s) and apps, and services by students must be done under the supervision of a professional staff member.

Student-created web content, for web pages/site(s), and apps, and services are subject to Policy 5722 - School-Sponsored Student Publications and Productions.

Purpose of Content of Corporation Web Pages/Site(s), Apps and Services

The Superintendent shall have final editorial authority over all content placed on the Corporation's servers or Corporationaffiliated servers and displayed on the Corporation's web pages/site(s), and/or apps and services. The Superintendent has the right to remove pages or links from any web page/site, as well as require that an app or service created by a Corporation staff member be removed from the Corporation's servers or Corporation-affiliated servers, based upon his/her determination that the content is inappropriate or is not accessible to individuals with disabilities.

The purpose of web content services and apps hosted by the Corporation on its servers or Corporation-affiliated servers is to educate, inform, and communicate. The following criteria should be used to guide the development of such content, services and apps.

A. **Educate**
Content provided should be suitable for and usable by students and teachers to support the curriculum and Corporation's Objectives as listed in the Corporation's Strategic Plan.

B. **Inform**
Content may inform the community about the school, teachers, students, or departments, including information about curriculum, events, class projects, student activities, and departmental policies.

C. **Communicate**
Content may communicate information about the plans, policies and operations of the Corporation to members of the public and other persons who may be affected by Corporation matters.

The information contained on the Corporation's web pages/site(s), and apps and services should reflect and support the Corporation's Mission Statement, Educational Philosophy, and the Academic Improvement Process.

When the content includes a photograph or information relating to a student, including Corporation-issued email accounts, the Corporation will abide by the provisions of Policy 8330 - Student Records.

All links included on the Corporation's web pages/site(s), and apps and services also must meet the above criteria and comply with State and Federal law (e.g. copyright laws, CIPA, Section 504, ADA, and COPPA). Nothing in this paragraph shall prevent the Corporation from linking the Corporation's web pages/site(s) and apps and services to 1) recognized news/media outlets, e.g., local newspapers' websites, local television stations' websites, or 2) to web pages/sites(s), and apps and services that are developed and hosted by outside commercial vendors pursuant to a contract with the Board. The Board recognizes that such third party web pages/sites(s), and apps and services may not contain age-appropriate advertisements that are consistent with the requirements of Policy 9700.01, AG 9700B, and State and Federal law.

Under no circumstances are Corporation-created web pages/site(s), and apps and services to be used for commercial purposes, political lobbying, or to provide financial gains for any employee or student. As part of this prohibition, of web pages/site(s), and apps and services contained on the Corporation's website shall not: 1) include statements or other items that support or oppose a candidate for public office, the investigation, prosecution or recall of a public official, or the passage of a tax levy or bond issue; 2) include a link to a website of another organization if the other website includes such a message; or 3) communicate information that supports or opposes any labor organization or any action by, on behalf of, or against any labor organization.

Under no circumstances are staff member-created web pages/site(s), services or apps, including personal web pages/sites, to be used to post student progress reports, grades, class assignments, or any other similar class-related material. Employees are required to use the Board-specified websites, services or apps (e.g., Canvas, Skyward) for the purpose of conveying information to students and/or parents.

Staff members are prohibited from requiring students to go to the staff member's personal web pages/sites (including but not limited to Facebook, Instagram, or Pinterest) to check grades, obtain class assignments and/or class-related materials, and/or to turn in assignments.

The content of school web pages/site(s) and services and apps should reflect an understanding that both internal and external audiences will be viewing the information.

School web pages/site(s), and services and apps must be located on Corporation-owned or Corporation-affiliated servers.

The Superintendent shall prepare administrative guidelines defining the rules and standards applicable to the use of the Corporation's web pages/site(s), and apps and services and the creation of web content, pages/site(s), and apps and services by staff and students.

The Corporation retains all proprietary rights related to the design of web pages/site(s), and services and apps that are hosted on Corporation-owned or Corporation-affiliated servers, absent written agreement to the contrary.

Students who want their classwork or information regarding their athletic endeavors, if applicable, to be displayed on the Corporation's web pages/site(s), and apps and services must have written parent permission and expressly license the display of those endeavors and any related photographs without cost to the Board.

Prior written parental permission is necessary for a student to be identified by name on the Corporation's website, web pages/site(s) and apps and services.

Website Accessibility

The Corporation is committed to providing individuals with disabilities an opportunity equal to that of individuals without disabilities to participate in the Corporation's programs, benefits, and services, including those delivered through electronic and information technology, except where doing so would impose an undue burden or create a fundamental alteration. The Corporation is further committed to ensuring individuals with disabilities are able to acquire the same information, engage in the same interactions, and enjoy the same benefits and services within the same timeframe as persons without a disability, with substantially equivalent ease of use; that they are not excluded from participation in, denied the benefits of, or otherwise subjected to discrimination in any Corporation programs, services, and activities delivered online, as required by Section 504 and Title II of the ADA and their implementing regulations; and that they receive effective communication of the Corporation's programs, services, and activities delivered online.

The Corporation adopts this policy to fulfill this commitment and affirm its intention to comply with the requirements of Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 and 34 C.F.R. Part 104, and Title II of the Americans With Disabilities Act of 1990, 42 U.S.C. 12131 and 28 C.F.R. Part 35, in all respects.

A. Technical Standards

The Corporation will adhere to the technical standards of compliance identified at www.ltschools.org. The Corporation measures the accessibility of online content and functionality according to the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG) 2.0 Level AA, and the Web Accessibility Initiative - Accessible Rich Internet Applications Suite (WAI-ARIA 1.1) for web content.

B. Web Accessibility Coordinator

The Board designates its Director of Communications as the Corporation's Web Accessibility Coordinator. That individual is responsible for coordinating and implementing this policy.

The Board commits to providing the Web Accessibility Coordinator with sufficient resources and authority to coordinate and implement this policy and any corresponding guideline(s), subject to oversight by the Superintendent and the Board.

The Corporation's Web Accessibility Coordinator can be reached at Director of Communications, www.ltschools.org, 317423-8375.

C. Third Party Content

Links included on the Board's web page/site(s), and apps and services that pertain to its programs, benefits, and/or services also must meet the above criteria and comply with State and Federal law (e.g., copyright laws, CIPA, Section 504, ADA, and COPPA). While the Corporation strives to provide access through its web pages/site(s) and apps and services to content provided or developed by third parties (including vendors, video-sharing websites, and other sources of online content) that is in an accessible format, that is not always feasible. The Corporation's administrators and staff, however, are aware of this requirement with respect to the selection of content provided to students. The Corporation's Web Accessibility Coordinator or his/her designees will vet content available on its web pages/site(s), and apps and services that is related to the Corporation's programs, benefits, and/or services for compliance with these criteria for all new content placed on the Corporation's web pages/site(s), and apps and services after adoption of this policy.

Nothing in the preceding paragraph, however, shall prevent the Corporation from including links on the Board's web pages/site(s) and apps and services to:

1. recognized news/media outlets (e.g., local newspapers' websites, local television stations' websites); or

2. web pages/sites, apps or services that are developed and hosted by outside vendors or organizations that are not part of the Corporation's program, benefits, or services.

The Board recognizes that such third party web pages/sites and apps and services may not contain age-appropriate advertisements that are consistent with the requirements of Policy 9700.01, AG 9700B, and State and Federal law.

D. Regular Audits

The Corporation, under the direction of the Web Accessibility Coordinator or his/her/their designees, will audit at regular intervals the Corporation's online content and measure this content against the technical standards adopted above.

This audit will occur no less than once every two (2) years.

If problems are identified through the audit, such problems will be documented, evaluated, and, if necessary, remediated within a reasonable period of time.

E. Reporting Concerns or Possible Violations

If any student, prospective student, employee, guest, or visitor believes that the Corporation has violated the technical standards in its online content, she/he may contact the Web Accessibility Coordinator with any accessibility concerns. She/He also may file a formal complaint utilizing the procedures set out in Board Policy 2260 and Policy 2260.01 relating to Section 504 and Title II.

Instructional Use of Apps, and Services

The Board authorizes the use of apps, and services to supplement and enhance learning opportunities for students either in the classroom or for extended learning outside the classroom.

The Board requires the Chief Technology Officer pre-approve each app or service that a teacher intends to use to supplement and enhance student learning. To be approved, the app or service must have a FERPA-compliant privacy policy and comply with all requirements of COPPA and CIPA and Section 504 and the ADA.

The Board further requires the use of a Corporation-issued e-mail address in the login process.

Training

The Corporation will provide annual training for its employees who are responsible for creating or distributing information through web pages/site(s) and apps and services so that these employees are aware of this Policy and understand their roles and responsibilities with respect to web design, accessibility, documents and multimedia content.
Such training shall be facilitated by an individual with sufficient knowledge, skill and experience to understand and employ the technical standards set forth in Board policies and administrative guideline(s).

One-Way Communication Using Corporation Web Pages/Site(s) and Apps and Services

The Corporation is authorized to use web pages/site(s) and apps and services to promote school activities and inform stakeholders and the general public about Corporation news and operations.

Such communications constitute public records that will be archived.

When the Board or Superintendent designates communications distributed via Corporation web pages/site(s) and apps and services to be one-way communication, public comments are not solicited or desired, and the web page/site, app or service is to be considered a nonpublic forum.

If the Corporation uses an app or service that does not allow the Corporation to block or deactivate public comments (e.g., Facebook, which does not allow comments to be turned-off, or Twitter, which does not permit users to disable private messages or mentions/replies), the Corporation's use of that app or service will be subject to Policy 7544 - Use of Social Media, unless the Corporation is able to withhold all public comments automatically.

If unsolicited public comments can be withheld automatically, the Corporation will retain the comments in accordance with its adopted record retention schedule (see AG 8310A – Requests for Public Records and AG 8310E - Record Retention and Disposal), but it will not review or consider those comments.

Revised 5/22/17

Legal

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

15 U.S.C. 6501 et seq., Children's Online Privacy Protection Act

20 U.S.C. 6777, 9134

47 U.S.C. 254, Communications Act of 1934, as amended

34 C.F.R. Part 99, Family Educational Rights and Privacy Act

47 C.F.R. 54.520, Children's Internet Protection Act

Book	Policy Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	Active
Adopted	November 16, 2015
Last Revised	February 28, 2022

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

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

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

Users are prohibited from engaging in 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) when using Corporation Technology Resources. Because its Technology Resources are not unlimited, the Board also has 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 Corporation 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 Corporation's computer network and/or Internet connection).

First, the Corporation may not be able to limit access technologically, through its Technology Resources to only those services and resources 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.

The Board prohibits the sending, receiving, viewing, or downloading of materials that are harmful to minors on computers and other technology related devices owned or leased by the Corporation or connected to the Corporation computer network.

Pursuant to State and 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 or IC 35-49-2-2. At the discretion of the Board or the

Superintendent, the technology protection measures may 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 students 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 Corporation 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 Superintendent or Chief Technology Officer may temporarily or permanently unblock access to websites or online education services/apps containing appropriate material, if access to such sites has been blocked inappropriately 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.

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

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

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

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

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

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

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

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

Building principals are responsible for providing training so that Ed-Tech 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 Corporation Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media and in chat rooms, and cyberbullying awareness and response. Users of Corporation 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, peers, and individuals and/or organizations outside the Corporation with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned email account when signing up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

Students are responsible for good behavior when using Corporation Technology Resources - i.e., behavior comparable to that expected of students when they are in classrooms, in school hallways, on other school premises and at school sponsored events. Communications on Education Technology are often public in nature. General school rules for behavior and communication apply. The Corporation does not approve any use of its Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

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

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

The Board designates the Superintendent and Chief Technology Officer as the administrator(s) responsible for initiating, implementing, and enforcing this Policy and its accompanying guidelines as they apply to students' use of Corporation Technology Resources.

This policy shall be posted on the Corporation's website.

Revised 5/14/18

Legal	P.L. 106-554 (2000), Children's Internet Protection Act of 2000
	47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
	18 U.S.C. 1460
	18 U.S.C. 2246
	18 U.S.C. 2256
	20 U.S.C. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
	20 U.S.C. 6777, 9134 (2003)
	47 C.F.R. 54.500 - 54.523
	I.C. 35-49-2-2
	I.C. 20-26-5-40.5

Book	Policy Manual
Section	7000 Property
Title	STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.04
Status	Active
Adopted	November 16, 2015
Last Revised	February 28, 2022

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

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

The Board regulates the use of Corporation Technology Resources and Information Resources by principles consistent with applicable local, State, and Federal laws, and the Corporation's educational mission. This policy, its related administrative guidelines and any applicable employment contracts and collective bargaining agreements govern the staffs' use of the Corporation's Technology Resources and Information Resources and staff's personal communication devices when they are connected to the Corporation's computer network, Internet connection and/or online educational services/apps, or when used while the staff member is on Corporation-owned property or at a Corporation-sponsored activity (see Policy 7530.02).

Users are prohibited from engaging in 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) when using Corporation Technology Resources and Information Resources. Because its Technology Resources are not unlimited, the Board also has 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 Corporation Technology Resources 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 Corporation's computer network and/or Internet connection).

Staff members are expected to utilize Corporation Technology Resources 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 in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy 2520 – Selection of Instructional Materials and Equipment.

The Internet is a global information and communication network that provides students and staff with access to up-to-date, highly relevant information that will enhance their learning and the education process. Further, Corporation Technology Resources provide students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

The Corporation may not be able to limit access technologically through its Technology Resources to only those services and resources 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 which may not have been screened by educators for use by students of various ages.

The Board prohibits the sending, receiving, viewing, or downloading of materials that are harmful to minors on computers and other technology related devices owned or leased by the Corporation or connected to the Corporation's computer network.

Pursuant to State and Federal law, the Corporation 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 or I.C. 35-49-2-2. At the discretion of the Board or Superintendent, the technology protection measures may 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 students 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 Corporation 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 Superintendent or Chief Technology Officer may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been blocked inappropriately 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 Superintendent or Chief Technology Officer may also disable the technology protection measures to enable access for bona fide research or other lawful purposes.

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

A. the safety and security of students while using e-mail, chat rooms, social media, 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 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 use of technology 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 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 Corporation Technology Resources. All users of Corporation Technology Resources 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, parents, and other staff members.

With prior approval from the Superintendent or Chief Technology Officer, staff may direct students who have been issued schoolassigned 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 on Corporation Technology and Information Resources, i.e., behavior comparable to that expected when they are in classrooms, in school hallways, on other school premises and at school-sponsored events. Communications on Education Technology are often public in nature. The Board does not approve any use of its Technology Resources and Information Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Staff members may use Corporation Technology Resources to access or use social media only if it is done for Corporation educational or business-related purposes.

General school rules for behavior and communication apply.

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

The Board designates the Superintendent and the Chief Technology Officer as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of Corporation Technology and Information Resources.

Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments related to matters of private concern that could compromise the Corporation'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 parent consent (see Board Policy 8330). Education records include a wide variety of information, and 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 student or employee information may be disciplined.

Nothing in this policy is intended to interfere with any school employee's rights under applicable law with respect to union organizing or collective bargaining.

This policy shall be posted on the Corporation's website.

Revised 5/14/18

Legal

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

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6301 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

20 U.S.C. 6777, 9134 (2003)

47 C.F.R. 54.500 - 54.523

I.C. 20-26-5-40.5

I.C. 35-49-2-2

Book

Section

Title CORPORATION-ISSUED STAFF E-MAIL ACCOUNT

Code po7540.05

Status Active

Adopted May 14, 2018

7540.05 - CORPORATION-ISSUED STAFF E-MAIL ACCOUNT

Staff

The School Board is committed to the effective use of electronic mail ("e-mail") by all School Corporation staff and Board members in the conduct of their official duties. This policy and any corresponding guidelines 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.

When available, the Corporation's e-mail system must be used by employees for any official Corporation e-mail communications.

Corporation staff shall not send or forward mass e-mails, even if the e-mails concern Corporation business, without prior approval of the Chief Technology Officer.

Corporation staff may join list servs or other e-mail services (e.g. RSS feeds) that pertain to their responsibilities in the Corporation.

Staff members are encouraged 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 (see Policy 8315 – Information Management), and purging all other e-mails that have been read. If the staff member is concerned that his/her email storage allotment is not sufficient, s/he should contact the Corporation's IT staff.

Staff members are prohibited from using school email (or school time) to promote any referendum after the resolution is passed or any political candidates.

Nothing in this policy is intended to interfere with any school employee’s rights under applicable law with respect to union organizing or collective bargaining.

Public Records

The Corporation complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to Corporation staff and Board members may be public records if their content concerns Corporation business 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 must be maintained pursuant to Policy 8330 – Student Records. Finally e-mails may constitute electronically stored information ("ESI") that may be subject to a litigation hold 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 involving ESI.

E-mails written by or sent to Corporation staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns Corporation business or education records if their content includes personally identifiable information about a student. Consequently, staff shall comply with a Corporation 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 litigation hold, 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 Corporation.

Retention

Pursuant to State and Federal law, e-mails that are public records or education records and e-mails that are subject to a litigation hold shall be retained.

The Corporation maintains archives of all e-mails sent and/or received by users of the Corporation'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 Corporation server to their Corporation e-mail account so that these records also are archived for future retrieval, if necessary.

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 nonexistent 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 7540.04, staff and Board members using the Corporation's e-mail system shall acknowledge their review of, and intent to comply with, the Board policy on acceptable use and safety.

Furthermore, staff and Board members using the Corporation's e-mail system shall satisfactorily complete training on student internet safety, including use of email, pursuant to Policy 7540.04 and regarding the proper use and retention of e-mail annually.

Book

Section

Title CORPORATION-ISSUED STUDENT E-MAIL ACCOUNT

Code po7540.06

Status Active

Adopted May 14, 2018

7540.06 - **CORPORATION-ISSUED STUDENT E-MAIL ACCOUNT**

Students assigned a School Corporation-issued 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 Corporation with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their assigned Corporation-issued 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 students' proper use of e-mail as an educational tool.

Personal e-mail accounts on providers other than the Corporation'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 Corporation's network when opening or forwarding any emails 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 their classroom teacher or the Chief Technology Officer.

Students may join list servs or other e-mail services (e.g., RSS feeds) that pertain to academic work.

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 School 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 nonexistent 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 Corporation's e-mail system shall acknowledge their review of, and intent to comply with, the Corporation's policy on acceptable use and safety annually.

Furthermore, students using the Corporation's e-mail system shall satisfactorily complete training, pursuant to Policy 7540.03, regarding the proper use of e-mail annually.

Policy Manual

7000 Property

Book	Policy Manual
Section	7000 Property
Title	ELECTRONIC DATA PROCESSING DISASTER RECOVERY PLAN
Code	po7541
Status	Active
Adopted	November 16, 2015

7541 – ELECTRONIC DATA PROCESSING DISASTER RECOVERY PLAN

The Board of School Trustees is committed to maintaining and protecting the Corporation's Information System. The Board believes that a complete and accurate Information System which includes educational, student, fiscal and personnel information is vital to the Board's ability to deliver uninterrupted educational service to the community it represents. To that end, the Superintendent, shall develop, test and maintain an Electronic Data Processing Disaster Recovery Plan for use in the event a disaster should disable the Corporation's electronic data processing equipment.

The Plan may include:

A. a reciprocal agreement with a neighboring school corporation or data acquisition site, which outlines the scope of reciprocal services such as access to the computer facility of the alternative, computer time and personnel assistance, and costs;

B. adequate equipment insurance;

C. a list of the applications that are used by the Corporation;

D. procedures used to backup all programs and data on a daily, monthly, quarterly and year-end basis;

E. backup storage off-site;

F. maintenance agreements for hardware and software (including, but not limited to the operating system);

G. a list of vendor contacts to be called for the immediate replacement of disabled equipment or corrupted software;

H. as a last resort, the procedure to create payroll checks and budgetary checks, and perform other necessary accounting functions, manually;

Policy Manual

7000 Property

4/12/22, 10:03 PM

Book

Section

Title	ACCESS TO CORPORATION TECHNOLOGY RESOURCES FROM PERSONAL COMMUNICATION DEVICES
Code	po7542
Status	Active
Adopted	November 16, 2015

7542 - **ACCESS TO CORPORATION TECHNOLOGY RESOURCES FROM PERSONAL COMMUNICATION DEVICES**

The Board permits employees, students, Board members, and guests, to use their personal communication devices ("PCDs") to wirelessly access the Corporation's technology resources (guest or business networks, servers, projectors, printers, etc.) while they are on-site at any Corporation facility. Access to the business/guest network shall require authentication.

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 phone (e.g., mobile/cellular telephones, smartphones (e.g., BlackBerry, iPhone, etc.), and/or other web-enabled devices of any type.

The standards shall be designed and enforced to minimize the Board's exposure to damages, including, but not limited to, the loss of sensitive Corporation data, illegal access to confidential data, damage to the Corporation's intellectual property, damage to the Corporation's public image, and damage to the Corporation's critical internal systems, from unauthorized use.

The use of PCDs must be consistent with the established standards for appropriate use as defined in Policy 7540.03 and AG 7540.03 – Student Network and Internet Acceptable Use and Safety, Policy 7540.04 and AG 7540.04 – Staff Network and Internet Acceptable Use and Safety, Policy 5136 and AG 5136 - Personal Communication Devices, Policy 7530.02 - Staff Use of Communication Devices. When an individual connects to and uses the Corporation’s technology resources, s/he must agree to abide by all applicable policies, administrative guidelines and laws (e.g., the user will be presented with a "splash screen" that will set forth the terms and conditions under which s/he will be able to access the Corporation’s technology resource(s); the user will need to accept the stated terms and conditions before being provided with access to the specified technology resource(s)).

In order to comply with the Children’s Internet Protection Act ("CIPA"), 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. The Board also utilizes software and/or hardware to monitor online activity to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors.

Any user who violates the established standards and/or the Board's Acceptable Use policy, or who accesses the Corporation’s technology resources without authorization may be prospectively denied access to the Corporation’s technology resources. If the violation is committed by a contractor, vendor or agent of the Corporation, the contract may be subject to cancellation. Further disciplinary action may be taken if the violation is committed by a student or employee.

The owner of a PCD bears all responsibility and assumes all risk of theft, loss, or damage to, or misuse or unauthorized use of the device while it is on Board property. This provision applies to everyone, regardless of their affiliation or connection to the Corporation.

Book

Section

Title	REMOTE ACCESS TO THE CORPORATION'S NETWORK
Code	po7543
Status	Active
Adopted	November 16, 2015

7543 - **REMOTE ACCESS TO THE CORPORATION'S NETWORK**

Access to the Corporation's Website (www.Itschools.org) is encouraged.

The following resources shall be available on the Corporation's website:

A. the Corporation's calendar of events

B. (gradebook program)

C. (required State report)

D. Board agendas and minutes

The Board encourages employees, parents, students, and community members to check the Corporation's website regularly for changes to these resources and for the addition of other resources. Some resources may require a user name and password, or a login procedure due to the personally identifiable nature of the information provided through that resource (e.g., the gradebook program and e-mail system). If a user name and password, or login procedure, is necessary to access a resource, information shall be provided on the website explaining who is eligible for a user name and password, how to obtain a user name and password, and detailed instructions concerning the login process.

Board members, Corporation employees, students and guests are permitted to use their personally-owned or Corporationowned computer or workstation and/or web-enabled devices of any type to remotely (i.e. away from Corporation property and facilities) access the Corporation's server and thereby connect to the Corporation's Network. This policy is limited to remote access connections that are used to do work on behalf of or for the benefit of the Corporation, including, but not limited to, reading or sending e-mail and reviewing Corporation-provided intranet web resources and completing assigned coursework.

Each individual granted remote access privileges pursuant to this policy must adhere to the following standards and regulations:

A. his/her device computer/device must have, at the minimum, the anti-virus software specified in the Corporation's standards for remote access and connection

B. the individual may only access the Network using his/her assigned user name and password

The individual must not allow other persons, including family members, to use his/her user name and password to login into the Network. The user may not go beyond his/her authorized access.

C. his/her device may not be connected to any other network at the same time s/he is connected to the Network, with the exception of personal networks that are under the complete control of the user

D. the individual may not access non-Corporation e-mail accounts (e.g. Hotmail, Gmail, Yahoo, AOL, and the like) or other external resources while connected to the Network

E. his/her device may not, at any time while the individual is using remote access to connect to the Network, be reconfigured for the purpose of split tunneling or dual homing

F. use of the Network is contingent upon the individual abiding by the terms and conditions of the Corporation's Network and Internet Acceptable Use and Safety policy and guidelines

Users may be required to sign the applicable agreement form (Form 7540.03 F1 or Form 7540.04 F1) prior to being permitted to use remote access.

Additional standards and regulations for remotely accessing and connecting to the Corporation network shall be developed and published in AG 7543 - Standards and Regulations for Remote Access and Connection.

Any user who violates this policy may be denied remote access and connection privileges.

Any employee who violates this policy may be disciplined, up to and including termination; any contractor, vendor, agent and guests who violates this policy may have his/her contract with the Corporation terminated; and any student who violates this policy may be disciplined up to and including suspension or expulsion.

4/12/22, 10:11 PM
Book

Section	8000 Operations
Title	CONTINUITY OF ORGANIZATIONAL OPERATIONS PLAN
Code	po8300
Status	Active
Adopted	May 14, 2018

8300 - **CONTINUITY OF ORGANIZATIONAL OPERATIONS PLAN**

The Continuity of Organizational Operations Plan (COOP) provides the School Corporation 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 Corporation'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 Corporation'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 Corporation 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 Corporation.

The Corporation-wide plan describes how the Corporation 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 Corporation's operations requires the cooperative efforts of external organizations, in partnership with the functional areas supporting the business of the Corporation. This includes local government agencies, law enforcement, emergency management, medical services, and vendors necessary to Corporation operations. The COOP outlines and coordinates all efforts by the Corporation in cooperation with other local and State agencies and businesses to restore the essential functions of the Corporation to the larger local community post-disaster.

The Superintendent shall recommend the COOP for Board 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.

Book	Policy Manual
Section	8000 Operations
Title	INFORMATION SECURITY
Code	po8305
Status	Active
Adopted	May 14, 2018
Last Revised	February 28, 2022

8305 - **INFORMATION SECURITY**

The School Corporation 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 Corporation. This information may be in hard copy or digital format, and may be stored in the Corporation or offsite with a third party provider.

Protecting Corporation data/information is of paramount importance. Information security requires everyone's active participation to keep the Corporation's data/information secure. This includes Board members, staff members/employees, students, parents, contractors/vendors, and visitors who use Corporation Technology and Information Resources. The Corporation will work to protect the data/information, computer network or system from attack vectors, or methods by which the computer network or system is attacked, infiltrated, or otherwise compromised.

A cybersecurity incident is a malicious or suspicious occurrence that consists of one (1) or more of the categories of attack vectors and are defined as applications, hardware or persons/organizations that:

A. jeopardize or may potentially jeopardize the confidentiality, integrity, or availability of an information system, an operational system, or the information that such systems process, store or transmit;

B. jeopardizes or may potentially jeopardize the health and safety of the public; or

C. violate security policies, security procedures, or acceptable use policies (See Policy7540.03 - Student Acceptable Use Policy/Policy 7540.04 - Staff Acceptable Use Policy)

A cybersecurity incident may consist of one (1) or more of the following categories of attack vectors: 1) ransomware; 2) business email compromise; 3) vulnerability exploitation; 4) zero-day exploitation; 5) distributed denial of service; 6) website defacement; or other sophisticated attacks as defined by the Chief Information Officer (CIO) and identified by the Corporation on its website.

Individuals who are granted access to data/information collected and retained by the Corporation must follow established procedures so that the information is protected and preserved. Board members, administrators, and all Corporation staff members, as well as contractors, vendors, and their employees, granted access to data/ information retained by the Corporation are required to certify annually that they shall comply with the established information security protocols pertaining to Corporation data/information. Further, all individuals granted access to Corporation Confidential Data/Information retained by the Corporation 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 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 safety and security of that data/information and the Corporation Technology Resources on which it is stored.

If an individual has any questions concerning whether this policy and/or its related administrative guidelines apply to him/her or how they apply to him/her, the individual should contact the Corporation's Technology Director or Information Technology Department/Office.

The Board authorizes the Superintendent to develop administrative guidelines that set forth the internal controls necessary to provide for the collection, classification, retention, access, and security of Corporation Data/Information. Within the established administrative guidelines, the Superintendent will determine a method for maintaining a repository of cybersecurity incidents.

Further, the Superintendent is authorized to develop procedures that would be implemented in the event of an unauthorized release of data/information. These procedures shall comply with the Corporation'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 Corporation Confidential Data/Information will be informed of relevant Board policies that govern access to and use of Corporation Information Resources, including the duty to safeguard the confidentiality of such data/information.

Failure to adhere to this Policy and its related administrative guidelines ("AGs") may put Corporation data/information 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 referred to the Corporation's disciplinary system and/or 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 Corporation. Parents and visitors who violate this Policy and/or AGs may be denied access to Corporation Technology Resources and/or referred to law enforcement.

The Superintendent shall conduct a periodic assessment of risk related to the access to and security of the data/information retained by the Corporation, as well as the viability of the Continuity of Organizational Operations Plan developed pursuant to Policy 8300.

Legal I.C. 4-13.1-1-1.3

I.C. 4-13.1-1-1.5

I.C. 4-13.1 -2-2

Book	Policy Manual
Section	8000 Operations
Title	PUBLIC RECORDS
Code	po8310
Status	Active
Adopted	November 16, 2015
Last Revised	January 13, 2020

8310 - **PUBLIC RECORDS**

The Board recognizes its responsibility to maintain and protect the public records of the Board and to make these records available for inspection and the purchase of copies in compliance with the Indiana Access to Public Records Act, I.C. 5-14-3-4 ("APRA").

"Public Records" Defined and Mandatory and Discretionary Exemptions

The public records of this Board are those records that are created, received, retained, maintained, or filed with the board or its officers, employees, or agents in any form including on paper and in any computer readable media. Certain records covered by this definition must be maintained as confidential records pursuant to I.C. 5-14-3-4(a) unless production is ordered by a court under the rules of pre-trial discovery, while other records covered by this definition are subject to a discretionary exemption listed in I.C. 5-14-3- 4(b).

Protection of Public Records

A person who recklessly, knowingly, or intentionally destroys or damages any public record commits a Class D felony in violation of I.C. 5-15-6-8. Public records may be destroyed when the Marion County Commission on Public Records created pursuant to I.C. 5-15- 6 has given written approval for the destruction of the record, or authority for destruction of the records is addressed by a retention schedule established and approved under I.C. 5-15-6.

Protection of Confidential Information in Public Records

As used in this policy, the term "redact" means to black out or cover with a permanent opaque material so that the content cannot be read. Where redaction is necessary, sufficient content shall be redacted so that the redacted content cannot be identified from the context.

The Board directs the Superintendent and Board employees having custody and supervision over public records to protect the confidentiality of records that are not to be disclosed under I.C. 5-14-3-4(a). This includes a person's Social Security Account Number ("SSAN") which shall be redacted from any public record released unless the SSAN is specifically required to be disclosed by a State or a Federal law or is ordered by a court under the rules of discovery.

Other information that must be kept confidential includes personally identifiable information about a student protected by the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g and 34 CFR Part 99, medical or genetic information about an employee, and information containing a trade secret as defined in I.C. 24-2-3-2.

Authorization to Assert Mandatory and Discretionary Exemptions

Given the time limitations established for compliance with a response to a request for records under the APRA, the Board directs the Superintendent to assert any exemption required to protect information that must be kept confidential pursuant to I.C. 5-14-3-4(a); and the Board authorizes the Superintendent to assert any discretionary exemption to the APRA found in I.C. 5-14-34(b) including: records that are intra-agency or inter-agency advisory or deliberative material; diaries, journals, or other personal notes serving as the functional equivalent of a diary or journal; files of applicants for Board employment, and personnel files of Board employees, except that the following information from personnel files must be disclosed:

A. the name, compensation, job title, business address, business telephone number, job description, education and training background, previous work experience, or dates of first and last employment of present or former officers or employees of the Board;

B. information relating to the status of any formal charges against a Board employee; and

C. the factual basis for a disciplinary action in which final action has been taken and that resulted in the employee being suspended, demoted, or discharged.

If personnel file information about a current or former employee is disclosed, the current or former employee shall be advised of the release of the information from their personnel file and a description of the released information.

Limited Access to Requests for Lists of Persons

Notwithstanding any other provisions of law or this policy, in compliance with I.C. 5-14-3-4(f), the Board will not create a new list or provide a copy of an existing list that includes the names and addresses of persons (including e-mail addresses) in response to a request unless the Board is required by law to publish and disseminate the list to the public.

However, if the Board has created a list of names and addresses of persons, it will permit a person to inspect and make memoranda abstracts from the list, excluding e-mail addresses unless access to the list is prohibited by law.

Requests for Lists of Employees or Students for Commercial or Political Purposes

When a list of employees and/or students is requested from the Corporation, notwithstanding the general prohibition of asking a requesting party for the purpose of their request, the requesting party will be required to disclose the proposed use of the list in writing, before their request is considered.

If the request is for:

A. a list of all employees of the Board, the employees in a particular school, a particular program, or classification of employee;

B. a list of persons attending conferences or meetings at a state educational institution or of persons involved in programs or activities conducted or supervised by the state educational institution;

C. a list of students who are enrolled in the Corporation, or sorted by any criterion or criteria;

and the proposed use of the list is for political or commercial purposes, the request shall be denied (see I.C. 5-14-3-3(f)).

For purposes of this policy, "political purposes" means influencing the election of a candidate for federal, state, legislative, local, or school board office or the outcome of a public question, or attempting to solicit a contribution to influence the election of a candidate for federal, state, legislative, local, or school board office or the outcome of a public question and "commercial purposes" means promotion of a product or service available from a business.

If all or any portion of a list of employees or student is disclosed, the party receiving the list shall be required to agree in writing that as a condition of release of the information, any information provided to them will not be used for political or commercial purposes. A person or entity that violates such a written agreement and any person or entity that used a list obtained through them shall not be eligible to receive lists of persons through the Board in the future. The Superintendent is directed to provide for consistent and uniform enforcement of this prohibition among all similarly situated commercial and political entities.

Lists of Students for Use by Official Recruiting Representative of Armed Forces

Notwithstanding any policy to the contrary, a request for a list containing "directory information" as defined at I.C. 20-33-10-3 and the Family Rights and Privacy Act ("FERPA") from an official recruiting representative of an armed force of the United States pursuant to I.C. 20-33-10 and/or 9528 of the ESEA (20 U.S.C. 7908), as amended by the No Child Left Behind Act of 2001 (P.L. No. 107-110), shall not be denied. However, an official recruiting representative may be required to pay a fee that represents the actual costs of copying and mailing the student directory information to the recruiter.

This information shall not be provided if a high school student or the parent of a high school student submits a signed, written request at the end of the student's sophomore year that states that the student or the parent of the student does not want the student's directory information to be provided to official recruiting representatives of the armed forces of the United States. Notice of the right to object to the release of student directory information generally under FERPA, and to official recruiting representatives of the armed forces of the United States, specifically, shall be provided in annual notices given to all high school students and their parents, guardian, or custodian.

A request to inspect and/or purchase copies of a public record in the custody of the Board may be submitted orally during the regular business hours in the office in which such records are maintained. A written request to inspect and make notes from public records in the custody of the Board may be submitted by e-mail, facsimile, or USPS mail. Such a request submitted outside of the regular business hours in the office in which such records are maintained, shall be received at the beginning of the next regularly scheduled work day in that office.

A requesting party shall be required to describe the records sought with reasonable particularity.

The Board Public Access Officer ("PAO") designated by the Superintendent or a Board employee acting at the discretion of the PAO will advise the requesting party whether any records specified in the request are available for inspection and copying. When the person making the request is physically present in a Board office, makes the request by telephone, or requests enhanced access to a record, a denial of disclosure occurs at the earlier of the time an employee of the Board refuses to permit inspection and copying of the requested record; or twenty-four (24) hours elapse after the request is received. When a request is made by mail, e-mail, or by facsimile, a denial of the request occurs at the earlier of the time a Board employee refuses to permit inspection and copying of the requested record or when seven (7) days have elapsed from the date the request was received by the Corporation.

The initial response to a request required by these time limitations does not need to be the final response of the Board to a request, but the initial response shall at least acknowledge receipt of the request and provide an initial assessment of the existence of records covered by the request. In preparing a final response of the Board following the initial response, the PAO shall comply with I.C. 5-14-3-7 and shall take into account the other duties to be performed by Board employees with custody of the requested record and shall not cause or permit a material interference with the regular discharge of the other functions or duties of the Corporation or its employees.

In order to assure the integrity of the data maintained on the Corporation's computer network, and protect the confidentiality of protected information maintained by the Corporation, the Board will not authorize enhanced access to public records on its computer network. However, records that are not confidential may be viewed by a requesting party in paper form printed out for inspection on paper by the PAO or a Board employee acting at the direction of the PAO.

Fees for Purchasing Copies of Public Records

Board public records may be inspected without charge. Purchase of copies of public records may be made upon payment of a fee. The Board establishes the following fee schedule for purchase of a copy of public records. These fees will be uniform for all purchasers.

Copies shall be prepared by a Corporation employee and provided to a requesting party upon payment of a fee which is the greater of:

A. ten cents ($0.10) per page for copies that are not color copies or twenty- five cents ($0.25) per page for color copies; or

B. the actual cost of copying the document.

"Actual cost" means the cost of paper and the per-page cost for use of copying or facsimile equipment and does not include labor costs or overhead costs.

Certification of document as a true and accurate copy of an original record in the custody of the Corporation, five dollars ($5.00).

The Board will charge a fee for providing a duplicate of a computer tape, computer disc, microfilm, or similar or analogous record system containing a public record in the custody of the Corporation. The fee shall not exceed the sum of:

A. the Corporation's direct cost of supplying the information in that form; and

B. the standard cost of selling the same information to the public in the form of a publication if the Corporation has published the information and made the publication available for sale.

In response to a request for public records, the Board shall charge a fee for any time spent searching records that are in electronic format when the search exceeds five (5) hours. There will be no charge for the first five (5) hours of a search. The fee for time beyond the first five (5) shall be the lesser of: 1) the hourly rate of the person making the search; or 2) twenty ($20) per hour. This hourly fee for searching for records in an electronic format applies only to time the person making the search actually spends searching the records in electronic format. No minimum fee shall be established. School personnel, doing an electronic search in response to a request for public records, will make a good faith effort to complete the search within a reasonable time in order to minimize the amount of the search fee. Any fee charged shall be prorated to reflect any part of the search which is less than a full hour. No charge will be made for "computer processing time." "Computer processing time" is defined as the amount of time a computer takes to process a command or script to extract or copy electronically stored data that is the subject of a public records request.

Legal I.C. 5-14-3, 5-15-6, 20-33-10

Book	Policy Manual
Section	8000 Operations
Title	INFORMATION MANAGEMENT
Code	po8315
Status	Active
Adopted	November 16, 2015
Last Revised	November 26, 2018

8315 - **INFORMATION MANAGEMENT**

The School Board recognizes its responsibility, in certain circumstances, to maintain information created, maintained or otherwise stored by the School Corporation outside the "records retention schedule". In such situations, a litigation hold procedure will be utilized to identify and preserve information relevant to a specific matter. All information falling within a litigation hold, which is under the control of the Corporation, must be preserved in a readily accessible form and cannot be disposed of under the records retention and disposal procedures. Failure to comply with a litigation hold notice may result in disciplinary action, up to and including possible termination.

Definitions

"Documents" includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained or translated if necessary.

"ESI" includes, but is not limited to, writings, drawings, graphs, charts, photographs, blueprints, sound recordings, images and other data or data compilations stored in any electronic media from which information can be obtained or translated if necessary. It includes, but is not limited to, e-mails, e-mail attachments, instant messages, word processing files, spreadsheets, pictures, application program and data files, databases, data files, metadata, system files, electronic calendar appointments, scheduling program files, TIFF files, PDF files, MPG files, JPG files, GIF files, network share files, internal websites, external websites, newsgroups, directories, security and access information, legacy data, audio recordings, voice mails, phone logs, faxes, internet histories, caches, cookies or logs of activity on computer systems that may have been used to process or store electronic data.

"Electronic media" includes, but is not limited to, hard drives (including portable hard disk drives "HDD's"), floppy drives, disaster recovery media, and storage media (including DVD's, CD's, floppy discs, Zip discs/drives, Jazz discs/drives, USB memory drives, jump disc/drives, flash discs/drives, keychain discs/drives, thumb discs/drives, smart cards, micro-film, backup tapes, cassette tapes, cartridges, etc.), accessed, used and/or stored on/in/through the following locations: networks and servers; laptop and desktop work computers; home and personal computers; other computer systems; backup computers or servers; archives; wireless communication devices as defined in Bylaw 0100; pagers; firewalls; audit trails and logs, printers; copiers; scanners; digital cameras; photographic devices; and video cameras and devices. Electronic media shall also include any item containing or maintaining ESI that is obtained by the Corporation for Board member or employee usage or that an employee uses for such purpose (even if privately owned by the Board member or employee) from the date this policy is adopted into the future.

Initiation and Removal of a "Litigation Hold"

The Board or the Superintendent may initiate a "litigation hold" under this policy. If the Superintendent initiates a " litigation hold," s/he or the Board's legal counsel will notify the Board of the reason the litigation hold was instituted and its scope. When implementing a litigation hold, the Board or Superintendent may utilize an Electronically Stored Information Team ("ESI Team"). The Board's legal counsel shall be involved in implementation of the litigation hold procedure.

A litigation hold shall remain in place until removed by the Board. A litigation hold may be removed when the litigation or administrative agency matter has been resolved or can no longer be initiated. Any information maintained under this policy shall fall back under the records retention schedule once the " litigation hold is removed.

The Superintendent shall develop administrative guidelines outlining the procedures to be followed by Board members and employees when initiating and implementing a litigation hold. This policy shall be posted on the corporation website.

Legal	Federal Rules of Civil Procedure 34, 37(f)
	Indiana Rules of Trial Procedure 34

Book	Policy Manual
Section	8000 Operations
Title	STUDENT RECORDS
Code	po8330
Status	Active
Adopted	November 16, 2015
Last Revised	August 10, 2020

8330 - **STUDENT RECORDS**

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

Student "personally identifiable information" ("PII") 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 whom the School Corporation reasonably believes knows the identity of the student to whom the education record relates.

A social security number of a student contained in the records of the Corporation may be disclosed if the record is specifically required by a State or a Federal Statute or is ordered by a court under the rules of discovery.

PII concerning students shall be protected against theft, unauthorized access, alteration, disclosure, misuse, or invasion of privacy. Unless specifically authorized by the Superintendent or produced pursuant to a request under the Indiana Access to Public Records Act, PII concerning students shall not be left unprotected, shared or transferred from Corporation records to any place not within the control of the Corporation. This includes any laptop computer or portable storage medium.

The Board is responsible for maintaining records of all students attending schools in this Corporation. In addition to records mandated by the Federal Government, the State of Indiana requires that the Corporation record or include in the official high school transcript for each high school student the following information:

A. attendance records

B. the students' latest ISTEP/GQE test results

C. any secondary level and postsecondary level certificates of achievement earned by the student

D. immunization information from the student's immunization record

E. any dual credit courses taken that are included in the core transfer library under I.C. 21-42-5-4

F. a functional workplace Spanish designation on the student's transcript if the student successfully completed a Spanish language course that meets the requirements of I.C. 20-32-4-12(b)

The Board also authorizes the collection of other student information including, but not limited to:

A. observations and ratings of individual students by professional staff members acting within their sphere of competency;

B. samples of student work;

C. information obtained from professionally acceptable standard instruments of measurement such as:

1. interest inventories and aptitude tests,

2. vocational preference inventories,

3. achievement tests,

4. standardized intelligence tests;

D. verified reports of serious or recurrent behavior patterns;

E. rank in class and academic honors earned;

F. psychological tests;

G. custodial arrangements.

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, and designated school personnel, who have a legitimate educational interest in the information, or to other individuals or organizations as permitted by law.

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" includes any student who is eighteen (18) years of age or older, or who is enrolled in a postsecondary institution regardless of his/her age.

In situations in which a student has both a custodial and a noncustodial parent, both shall have access to the student's educational records unless stated otherwise by court order. In the case of an eligible student, that is a student who is eighteen (18) years of age or older, parents will 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.

A "school official" is a person employed by the Board as an administrator, supervisor, teacher/instructor (including substitutes), school psychologist, therapist, or support staff member (including health or medical staff and law enforcement unit personnel); and a person serving on the Board. The Board further designates the following individuals and entities as "school officials" for purposes of FERPA:

A. persons or companies with whom the Board has contracted to perform a specific task (such as an attorney, auditor, insurance representative, or medical consultant);

B. school psychologists, whether employed by a special education cooperative, interlocal, joint services organization, or an outside contractor, for purposes of the referral, evaluation, and identification of students suspected to have a disability;

C. contractors, consultants, volunteers or other parties to whom the Board has outsourced a service or function otherwise performed by Board employees (e.g. a therapist, authorized information technology (IT) staff, and approved online educational service providers).

The above-identified outside parties must (a) perform institutional services or functions for which the Board would otherwise use its employees, (b) be under the direct control of the Board with respect to the use and maintenance of education records, and (c) be subject to the requirements of 34 C.F.R. 99.33(a) governing the use and re-disclosure of PII from education records.

Finally, 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) is also considered a "school official" for purposes of FERPA provided s/he meets the above-referenced criteria applicable to other outside parties. "Designated school personnel" may include but is not limited to employees or agents of an insurance carrier providing a defense to the Corporation or its employees or agents and Corporation legal counsel.

In the case of a health or safety emergency, "appropriate officials" include local or State law enforcement officials, D epartment of C hild Services (DCS) officials, trained medical personnel, and school administrators whose knowledge of PII in a student's education records is necessary to protect the health or safety of students or other persons on Corporation property. The term "school administrator" includes a principal, an assistant principal, a superintendent, and an assistant superintendent. The term "school administrator" also includes a director of special education or assistant director of special education.

"Legitimate educational interest" shall be defined as a "direct or delegated responsibility for helping the student achieve one (1) or more of the educational goals of the Corporation" or if the record is necessary in order for the designated school personnel official to perform an administrative, supervisory or instructional task for the Corporation or to perform a service or benefit for the student or the student's

family or to provide a defense to the Corporation with respect to any of these tasks. 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 a 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 corporation in which a student of this Corporation 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 public school or school corporation in which a student in foster care is enrolled. Such records shall be transferred within one (1) school day of the enrolling school's request.

C. provide, disclose, or report on the education records of a student, including PII contained in the education records, without the consent of the student's parent or eligible student, to appropriate officials and the 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 school administrators determine there is an articulable and significant threat to the health or safety of a student or other individuals, considering the totality of the circumstances;

    Information concerning any suspicious activity or potential criminal activity related to a child that is shared between a law enforcement officer and the Corporation or an appropriate official shall not be stored or maintained in any type of database.

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

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. disclose personally identifiable information from education records, without consent, to organizations conducting studies "for, or on behalf of" the Corporation 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(s) 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 Corporation will enter into a written agreement with the recipient organization that specifies the purpose of the study. (See Form 8330 F14) Further, the following personally identifiable information will not be disclosed to any entity: a student or his/her family member's social security number(s); religion; political party affiliation; voting history; or biometric information.

    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 (other than social security numbers, religion, political party affiliation, voting record, or biometric information) is allowed under this exception, it is recommended that de-identified information be used whenever possible. This reduces the risk of unauthorized disclosure.

G. disclose personally identifiable information from education records without consent, to authorized representatives of the Comptroller General, the Attorney General, and the Secretary of Education, 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).

The Corporation will verify that the authorized representative complies with FERPA regulations.

H. disclose or report educational records to a State or local juvenile agency when the disclosure or reporting relates to the ability of the juvenile justice system to serve, before adjudication, the student whose records are being released; and the juvenile justice agency receiving the information certifies, in writing, that the agency or individual receiving the information has agreed not to disclose it to a third party, other than other juvenile justice agency, without the consent of the child's parent, guardian, or custodian.

   A disclosure or reporting of educational records concerning a child who has been adjudicated as a delinquent child shall be treated as related to the ability of the juvenile justice system to serve the child before adjudication if the agency provides documentation to the Corporation that the agency seeks the information in order to identify and intervene with the child as a juvenile at risk of delinquency rather than to obtain information solely related to the supervision of the child as an adjudicated delinquent child.

The juvenile court may grant a school access to all or a portion of the juvenile court records of a child who is a student at the school if the Superintendent submits a written request establishing that the juvenile court records are necessary for the school to serve the educational needs of the child whose records are requested or to protect the safety or health of a student, an employee, or a volunteer at the school.

The school shall keep the records confidential. However, the confidentiality order does not prohibit the school from forwarding the juvenile records to another school or a person if a parent, guardian, or custodian of the child consents to the release of the juvenile court records to the person.

The Corporation 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, 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 Corporation shall maintain a record of those persons to whom information about a student has been disclosed. Such disclosure records will indicate the student, person viewing the record, 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, the written consent of the student, except those persons or parties stipulated by the Corporation's policy and administrative guidelines and/or those specified in the law.

DIRECTORY INFORMATION

Each year, the Superintendent shall provide public notice to students and their parents of the Corporation's intent to make available, upon request, certain information known as "directory information". The Board designates as student "directory information": a student's name; address; telephone number; date and place of birth; major field of study; participation in officially recognized activities and sports; height and weight, if a member of an athletic team; dates of attendance; date of graduation; awards received.

The Board designates school-assigned email accounts as "directory information" for the limited purpose of facilitating students' registration for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes. School assigned email accounts shall not be released as directory information beyond this limited purpose and to any person or entity but the specific online educational service provider.

Directory information shall not be provided to any organization for profit-making purposes. The Superintendent may allow access to a school campus or give students' directory information to organizations that make students aware of educational or occupational options.

In accordance with Federal law, the Board shall comply with FERPA when releasing students' information to a recruiting officer for any branch of the United States Armed Forces or an institution of higher education who requests such information.

Parents and eligible students may refuse to allow the Corporation to disclose any or all of such "directory information" upon written notification to the Corporation within 10 days after receipt of the Superintendent’s annual public notice.

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 specifically stated otherwise by court order.

The Corporation may disclose "directory information" on former students without consent of the parent(s)/eligible student unless the parent or eligible student previously submitted a request that such information not be disclosed without their prior written consent.

Student Mental and Behavioral Health Services Records

Student Mental and Behavioral Health Services (SMBHS) records are documents relating to mental health or behavioral health services provided to students by 1) a provider certified or licensed by the State to provide mental or behavioral health services who is contracted or employed by the Corporation or a special education cooperative of which the Corporation is a member or 2) a community mental

health center established under State law with whom the Corporation or a special education cooperative of which the Corporation is a member has entered into a memorandum of understanding. SMBHS records include but are not limited to mental health records, reports, notes, diagnosis(es) and/or appointments relating to a student who was referred by Corporation officials to receive mental or behavioral health services pursuant to State law or under a memorandum of understanding between the Corporation and a community mental health center established under State law or a provider certified or licensed by the state to provide mental or behavioral health services to students. SMBHS records are to be considered medical records and are confidential. SMBHS records that include any reports, notes, diagnosis(es) or appointments that result from a student's participation in any treatment relating to mental or behavioral health services provided by a community mental health center or appropriate provider that is contracted and paid for by the Corporation or a special education cooperative of which the Corporation is a member shall not be maintained in a student's permanent educational file/cumulative file. SMBHS records kept by a provider employed or contracted by the Corporation or a special education cooperative of which the Corporation is a member shall be maintained in separate student folders in a secured file under the control of the provider. Sharing of any reports or notes resulting from a conference with the student and the student's parent to address the student's potential need for and benefit from mental or behavioral health services with other Corporation officials is strictly prohibited.

Disclosure of Lists of Students for Political or Commercial Purposes

It is the policy of the Board not to release the lists of students for commercial or political purposes. This policy shall be equally applied to similarly situated organizations and persons. (I.C. 5-14-3-3(f))

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 10 business days before the scheduled date of the activity. The instrument will be provided to the parent or eligible student within 5 business days of the principal receiving the request.

The Superintendent 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 Superintendent shall prepare procedures to 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 record is inaccurate, misleading, or otherwise in violation of the student's privacy rights;

C. consent to disclosures of personally-identifiable information contained in the student's education records, except disclosures allowed without parental consent;

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

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

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

The Superintendent also shall develop procedural guidelines for:

A. the proper storage and retention of records including a list of the type and location of records;

B. informing Corporation employees of the Federal and State laws concerning 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 Corporation specifically as a consequence of permitting access or furnishing students' records in accordance with this policy and administrative guidelines.

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 time frame for the activity has ended, as specified in its written agreement with the Board. See Form 8330 F14 and Form 8330 F16 for additional contract requirements.

Address Confidentiality Program

If a parent (or adult student) presents information to the Corporation certifying that the parent (or adult student), his/her child, or a member of the parent's household is a participant in the Address Confidentiality Program administered by the State Attorney General, the Corporation 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. Because student records are available to non-custodial parents, designated school officials who have a legitimate educational interest in the information, and other individuals or organizations as permitted by law (including the public in some situations), the Corporation shall list only the address designated by the Attorney General's Office to serve as the student's address in any student records or files, including electronic records and files. Further, the Corporation shall use the student's designated address for any and all communications and correspondence between the Board or Corporation employees 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 the student's actual/confidential residential address is prohibited. Any violations could result in disciplinary action.

Violation of this Policy

As provided for by State law, an employee or agent of the Board:

A. who knowingly or intentionally discloses information classified as confidential by State statute commits a Class A infraction;

B. who intentionally, knowingly, or recklessly discloses or fails to protect information classified as confidential by this policy may be disciplined or terminated.

Additionally, State law provides that a person who recklessly, knowingly, or intentionally destroys or damages any public record commits a Level 6 felony unless the destruction is pursuant to a record retention scheduled adopted by the County Public Records Commission.

Revised 11/28/16
Revised 5/22/17
Revised 11/21/17

Legal I.C. 5-14-3-3(f)
I.C. 5-14-3-4(a)(3) and (12)
I.C. 5-14-3-4(c)
I.C. 5-14-3-10
I.C. 5-15-6-8
I.C. 20-32-4-12
I.C. 20-33-2-13
I.C. 20-33-7-1 et seq.
I.C. 31-39-2-13.8
511 I.A.C. 7-38-1 et seq.
26 U.S.C. 152

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g

Individuals with Disabilities Education Act, 20 U.S.C. 1400 et seq.

20 U.S.C. 7165(b)

20 U.S.C. 7908

34 C.F.R. Part 99

34 C.F.R. Part 300

Book	Policy Manual
Section	8000 Operations
Title	SECURITY BREACH OF CONFIDENTIAL DATABASES
Code	po8351
Status	Active
Adopted	November 16, 2015

8351 - **SECURITY BREACH OF CONFIDENTIAL DATABASES**

It is the policy of the School Board that when unauthorized access or acquisition of data occurs, which would compromise the confidentiality or security of personal information maintained by the Corporation on a database, the Corporation will take appropriate action to assess the risk, and notify the affected individuals in accordance with law.

Scope

This policy applies to any security breach involving employees, consultants, vendors, contractors, outside agencies and employees of such agencies, and any other parties having a business relationship with the Corporation and handling personal information on the Corporation's behalf. It is expected that those offices, individuals or entities operating, maintaining, and using databases containing personal information will effectively control access to the databases to protect against unauthorized access, acquisition, modification, use or disclosure of personal information.

In order to better protect personal information and facilitate the investigation of incidents of unauthorized access, employees shall not store professional confidential information on a personal computer, server or other data storage equipment not owned or maintained by the Corporation.

Security Breach and Personal Information – Definitions

A "security breach" means the unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by the Corporation and that:

A. causes a material risk of identity theft or other fraud to the person or property of a resident of the State;

B. reasonably is believed to have caused a material risk of identity theft or other fraud to the person or property of a resident of the State; or

C. reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of the State.

Unauthorized access of information will not be considered a security breach if:

A. the employee or agent acted in good faith in accessing the data;

B. the access was related to the activities of the Corporation or the employee's or agent's job-related duties; and

C. the employee or agent did not use the personal information for an unlawful purpose or subject the information to further unauthorized disclosure.

Also, the acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant subpoena, order or duty of a regulatory State agency, will not be considered a security breach.

For purposes of this policy, personal information means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any of or more of the following (when the information is not encrypted, redacted, or altered by any method or technology in such a manner that the information is effectively obscured or unreadable):

A. Social Security number;

B. driver's license number or State identification card number; and/or

C. account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Discovery of Security Breach and Notification

If an employee suspects, discovers and/or determines that a security breach has occurred, the employee shall promptly notify his/her immediate supervisor and the Superintendent, in writing.

The Superintendent shall determine and implement the steps necessary to correct the unauthorized access and requirements for notifying those individuals whose personal information may have been compromised.

The Superintendent shall develop and implement administrative guidelines related to this policy.

METROPOLITAN SCHOOL DISTRICT
LAWRENCE TOWNSHIP

Book	Policy Manual
Section	8000 Operations
Title	AUTHORIZATION FOR AUDIO, VIDEO, AND DIGITAL RECORDING
Code	po8355
Status	Active
Adopted	May 14, 2018

8355 - **AUTHORIZATION FOR AUDIO, VIDEO, AND DIGITAL RECORDING**

The School Board believes that the education of children is a joint responsibility, one it shares with the parents and other members of the school community. The Board realizes it has the responsibility of protecting the rights of students in keeping and sharing student records and maintaining the confidentiality of personally identifiable student information under the Family Educational Rights and Privacy Act and State law.

Any person wishing to make any audio, video or digital recording or other recording by electronic means on school premises, with the exceptions listed below, shall obtain the permission of the Superintendent and the Building Principal prior to any recording.

Exceptions:

Any audio, video or digital recording authorized pursuant to Board Policy 2410 - Audio, Video, and Digital Recording of Meetings is not subject to additional authorization requirements under this policy.

The requirements of this policy shall not be interpreted to conflict with the provisions of Policy 5136 - Personal Communication Devices as it pertains to recordings. Nor shall the requirements of this policy be interpreted to extend to school-sponsored public events, where there can be no expectation of privacy. A school-sponsored public event is any school-related activity, whether free or at which an admission fee is charged, that members of the public may attend. These include but are not limited to athletic competition, plays, musical performances, awards ceremonies, and graduation. See Policy 9160 - Public Attendance at School Events for additional information about restrictions on recording at such events.

Legal I.C. 20-33-7

Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and 34 C.F.R. Part 99