Book	Policy Manual
Section	800 Operations
Title	Electronic Searches
Code	831
Status	Second Reading
Adopted	January 9, 2025

Purpose

The Board recognizes that many facets of modern technology hold private details such as photographs, communications, health information, Internet browsing history, and financial information that most individuals want to keep confidential.

The purpose of this policy is to establish guidelines for the search and seizure of electronic devices and online communications in the school district in order to maintain a safe and secure learning environment for all students, staff, and visitors while complying with the district's legal obligations. This policy applies to all electronic devices and online communications owned, operated, or controlled by the school district, as well as to personal devices and online communications that are used on school property or in connection with school-related activities.

Delegation of Responsibility

The Superintendent is responsible for the overall implementation and enforcement of this policy.

The **Technology Leader** is responsible for overseeing the technical aspects of electronic searches and ensuring that they are conducted in compliance with this policy and applicable laws and regulations.

Building principals are responsible for enforcing this policy within their respective buildings and ensuring that staff and students are aware of the policy.

Definitions

District technology resources means all technology owned, operated, and/or licensed by the district, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, applications, routers, and networks, including the Internet.

Electronic device - any device that can be used for storing, transmitting, or receiving electronic communications, including but not limited to computers, laptops, tablets, smartphones, and servers.

Electronic search - the examination, inspection, or retrieval of electronic data, content, or information stored on or transmitted through district technology resources or electronic devices, including but not limit to the examination of e-mails, files, photographs, videos, devices usage, and browsing history, conducted by authorized school personnel for legitimate educational or administrative purposes.

Online communication - any communication that is transmitted or received electronically, including but not limited to e-mail, instant messaging, social media, text messaging and any other electronic means of exchanging information.

Reasonable suspicion - a belief that is based on specific facts and articulable circumstances that would lead a reasonable person to conclude that a particular individual is involved in conduct that violates the law, the rules of the school, or school district policy.

Guidelines

Privacy

The district reserves the right to monitor any user's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy, and review any and all usage of district technology resources including information transmitted and received via the Internet to ensure compliance with this and other district policies, and state and federal law. All e-mails and messages sent through district technology resources, as well as any files stored on district technology resources, may be inspected at any time for any reason. The district may decrypt and inspect encrypted internet traffic and communications to ensure compliance with this policy and federal law.[1][2]

Requests for Searching District Technology Resources

The building principal, or other authorized administrator, shall submit a written request to the **Superintendent** for authorization to search a specific electronic device or account. The request shall include the specific facts and circumstances that form the basis for the reasonable suspicion that the electronic device or account contains evidence of a violation of the law, the rules of the school, or school district policy.

The **Superintendent** shall review the request and determine whether there is reasonable suspicion to authorize the search. If the **Superintendent** determines that there is not reasonable suspicion, the request shall be denied and the matter shall be closed.

Electronic searches of district technology resources may also be authorized by the **Superintendent** based upon reasonable suspicion that the electronic device or account contains evidence of a violation of the law or the rules of the school.

Reasonable suspicion includes notifications of suspicious content from monitoring software, or notification from staff or administrators of suspicious activity.

If the **Superintendent** authorizes the search, the search shall be conducted in accordance with this policy and applicable laws and regulations. If the **Superintendent** has authorized a search of a district device, all staff, students, and administrators shall promptly produce such devices upon request to the **Technology Leader**.

The **Technology Leader** shall take reasonable steps to preserve the integrity of the electronic device or account prior to and during the search.

The **Technology Leader** shall conduct the search in a manner that minimizes the intrusion on any individual's limited privacy rights, without jeopardizing the integrity of the search. The search must be proportionate to the specific, articulable facts that caused the reasonable suspicion.

The **Technology Leader** shall document the search, including the specific electronic device or account searched, the date and time of the search, and the reason for the search.

Any evidence of a violation of the law, the rules of the school, or school district policy discovered during the search shall be turned over to the appropriate law enforcement or school officials, who shall determine whether further action is necessary.

Supervising Students Engaged in Online Learning

Administrators and teachers responsible for supervising students engaged in online learning may monitor students' online activities including log in times, Internet browsing history, device usage, and other online activities. Such monitoring shall not be considered a search subject to the guidelines above, but rather constitutes routine monitoring of students in their learning environment.

Supervising Students Engaged in Classroom Learning

Administrators and teachers responsible for supervising students engaged in classroom learning may monitor students' classroom behavior, including the online activities of students in their classroom. They may also review application data and file version histories to ensure academic integrity. Such monitoring shall not be considered a search subject to the guidelines above, but rather constitutes routine monitoring of students in their learning environment.

Using Geolocation Tools

Only the **Technology Leader** can approve the use of geolocation features to identify the precise location of an electronic device owned by the school district. Geolocation is authorized whenever the **Technology Leader** is notified that a device is missing or stolen. The **Technology Leader** may approve the use of geolocation for other legitimate governmental purposes with approval by the Superintendent.

Exigency Exception

In the event of an urgent emergency posing a threat to the safety, security, or well-being of individuals within the school community or the integrity of school property, an exigency exception to this electronic search policy or administrative regulations may be invoked.

Under such emergency circumstances, school administrators or security personnel may conduct electronic searches without following the guidelines above.

This exception allows for swift action to mitigate risks and address imminent danger to the district and school community.

While the exigency exception grants broader authorization for electronic searches, such searches must remain proportionate to the exigent circumstances and are conducted with due regard for students' limited privacy rights. All actions taken under the exigency exception must be documented promptly and reported promptly to the Superintendent.

Development of Administrative Regulations

The Superintendent or his/her designee may develop administrative regulations to implement this policy. The Superintendent shall ensure that all students and employees are made aware of this policy and any administrative regulations by means of the employee and student handbooks, the school district website, or other reasonable means.

Legal	Pol. 815
	47 CFR 54.520
	Pol. 801
	Pol. 237
	N.J. v T.L.O. 468 U.S. 1214 (1984)
	Pol. 805.1
	Pol. 800
	Pol. 801
	Pol. 226
	22 PA Code 12.14
	24 P.S. 510
	Commonwealth v. Cass, 551 Pa. 25, 709 A.2d 350, 355-56 (1998)
	In re F.B., 555 Pa. 661, 726 A.2d 361, 368 (1999)
	Safford Unified School Dist. No. 1 v. Redding, 129 S.Ct. 2633 (U.S. 2009)
	PA Const. Art. I
	U.S. Const. Amend. IV
Cross References	Pol. 805 Emergency Preparedness and Response
	Pol. 227 Controlled Substances / Paraphernalia
	Pol. 218.1 Weapons
	Pol 223 Use of Bicycles and Motor Vehicles