

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

R142 K-12 TECHNOLOGY: SAFETY, MONITORING AND PRIVACY

I. Purpose

These administrative regulations establish expectations and procedures in order to support the implementation of Policy 142 and to ensure that Technology Resources are used safely and responsibly for Educational Purposes, reflecting a developmentally appropriate, balanced approach across grades K-12 that prioritizes non-digital learning experiences, engagement, and well-being of students in accordance with Policy and Administrative Regulation 141 (K-12 Technology Use).

II. Defined Terms

For purposes of implementing Policy 142 and this related Administrative Regulation, the following terms apply:

- **District Technology Resources (sometimes just referred to as Technology Resources):** All District-owned or District-approved technology systems, including:
 - All networks, servers and telecommunications systems maintained or operated by the District;
 - All District telephone, cellular phone, voicemail, electronic mail, intercom, and Internet resources;
 - All District-owned or issued hardware devices such as computers, laptops, tablets, telephones, cellular phones, drones, fax machines, printers, copiers, scanners, etc. (inclusive, but not limited to District-Issued Devices);
 - All web-based and cloud-based storage; and,
 - Web and cloud-based applications provided by the District through a third party.
- **District-Issued Devices:** Any device provided by the District for student use for an Educational Purpose, including laptops, tablets, or similar equipment. These devices remain District property at all times.
- **Educational Purpose:** Use that directly supports curriculum, teaching, learning, school-sponsored student activities, school-related communication, or school-related responsibilities. This includes research, content creation, collaboration, and instructional activities aligned to curriculum goals. This also includes use in support of specialized educational plans that provide inclusion and access.

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

- **Active Use (of Technology Resources):** Such use engages critical thinking through creation, problem-solving, design, collaboration, and interaction with others.
- **Passive Use (of Technology Resources):** Such use involves consuming content without reflection, creativity, or participation.
- **Digital Citizenship:** The responsible, ethical, and safe use of technology, including respectful communication, protection of personal information, appropriate online behavior, and adherence to academic integrity standards.
- **Monitoring:** The District's ability to review, track, or access activity on its technology systems and devices to ensure safety, security, and compliance with policy. Users should have no expectation of privacy when using District technology resources.
- **Filtering:** Technology protections that limit access to content that is harmful, inappropriate, or not aligned with educational purposes, in compliance with applicable laws.

III. Safety, Monitoring, and Privacy

The following procedures establish the District's operational practices for implementing Board Policy 142 and applicable federal and state law regarding student technology safety, monitoring, privacy, and responsible technology use.

A. Internet Filtering

The District is committed to protecting students while using District Technology Resources and internet access. To support this commitment, the District utilizes internet filtering and monitoring technologies designed to block or restrict access to obscene material, pornography (including child pornography), and other visual depictions that are harmful to minors, as defined by the Children's Internet Protection Act (CIPA).

The District also complies with the Children's Online Privacy Protection Act (COPPA) by taking steps to protect the privacy of students under the age of 13 when using online educational services and applications. The District evaluates digital resources to ensure that student data is collected, used, and shared only for legitimate educational purposes and in accordance with applicable laws.

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.:	142
Section:	PROGRAMS
Title:	K-12 TECHNOLOGY: SAFETY, MONITORING AND PRIVACY
Date Adopted:	8/17/26

In addition, the District complies with the Family Educational Rights and Privacy Act (FERPA) by safeguarding student education records and personally identifiable information. Vendors and service providers handling student information are required to maintain appropriate privacy and security protections consistent with applicable federal and state law.

These filtering and privacy protections represent the District's minimum requirements. The District will make reasonable efforts to restrict access to content that is not educationally relevant, curriculum-based, or appropriate for the school environment. The District continually reviews and updates its filtering and monitoring systems to enhance student safety and maintain compliance with applicable laws.

Staff, students, and parents/guardians are advised, however, that no filtering software is completely secure or effective. Merely because a technology protection measure does not prevent access to a particular site or to particular materials does not indicate that the site or the materials are appropriate. Together with District-provided Digital Citizenship instruction, the District encourages parents/guardians to specify to their child(ren) what material is and is not acceptable to access through District Technology Resources, within the parameters of this Administrative Regulation and the accompanying Board Policy.

The District is limited in its ability to filter material when a student accesses the internet from a source other than the District's Network and disclaims any responsibility for material accessed in that manner. However, the District reserves the right to discipline any student for intentionally accessing or possessing inappropriate, illegal, or otherwise prohibited or unauthorized material from whatever source obtained (including, but not limited to, circumventing the District's technology protection measures) on school property or for posting or distributing material to the District's Network or other District Technology Resource.

The Superintendent or designee may disable the technology protection measure if needed for bona fide research or another lawful purpose.

- **Student Request for Access to Blocked Materials**

Any student who claims that they have been denied access to Internet material needed for bona fide research that is not obscene material, child pornography or other visual depictions deemed harmful to minors shall be afforded expedited review and resolution of

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

this claim by making a written request to the teacher. The teacher shall forward the request via the helpdesk ticket system to the appropriate curriculum supervisor who shall respond to the request within a reasonable time under the circumstances not to exceed five (5) days. Only the Superintendent or Director of Information Technology and Cybersecurity may authorize the disabling of the technology protection measure to permit access.

B. Digital Application Review and Approval

To protect student privacy, ensure data security, and maintain compliance with applicable law, all digital applications, websites, and online services used with students shall undergo a District review and approval process before implementation.

The review process includes, but is not limited to:

- review of vendor privacy policies, terms of service, and data collection practices;
- evaluation of data minimization practices to ensure only information necessary for educational purposes is collected;
- assessment of information security controls, including encryption, access controls, incident response, and breach notification procedures;
- confirmation of compliance with FERPA, COPPA, CIPA, and other applicable laws;
- execution of a District-approved Data Privacy Agreement or equivalent contractual protections where required;
- evaluation of generative artificial intelligence (AI) applications for privacy, transparency, appropriate educational use, data retention, and compliance with District policies governing student information; and,
- periodic review of approved applications (including review following significant vendor changes, security incidents, or material revisions to privacy practices) to ensure continued compliance with evolving legal and security requirements.

Final approval of digital applications shall be made by the Director of Information Technology and Cybersecurity, or designee, in consultation with appropriate curriculum and instructional leaders.

C. Other Monitoring of District Technology Resources

- 1. General Monitoring:** The District reserves the right to conduct periodic general searches of files and communications shared, stored, or otherwise located on Technology Resources to determine whether inappropriate material, including copyrighted,

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

threatening or harassing material or material that threatens the operation or security of Technology Resources. Such general searches may be conducted by an Information Technology and Cybersecurity Department Professional as authorized by the Director of Information Technology and Cybersecurity. The District may remove or quarantine any files that it deems to be in violation of applicable law or District policy or that the District deems is a threat to the operation and security of the District Provided Technology Resources. If a student believes that a file has been removed in error, then the student may submit a written complaint to the Director of Information Technology and Cybersecurity, who shall review the complaint with appropriate District staff and make a determination as to whether the material should be returned to District Technology Resources, returned to the student, or be permanently deleted.

Employees shall promptly report suspected cybersecurity incidents, phishing attempts, unauthorized disclosure of District information Technology and Cybersecurity, or suspected compromise of District Technology Resources in accordance with District incident response procedures.

All student network shares or backup folders stored on technology resources located within the District's local network will be purged following the last day of classes for the school year.

- 2. Reasonable Suspicion:** If the District has a reasonable suspicion that a student is violating District rules or policies, authorized District administrators shall search a student's Technology Resources including, but not limited to electronic mail accounts, District-hosted or web-based or cloud-based storage and other web-based and cloud-based applications. "Reasonable suspicion" means that reasonable grounds exist that the search will uncover evidence that the student violated the law, school rules or District policies. The scope of the search must be reasonably related to the suspected violation which justified the search. Typically, the District will request that the student provide access to the account and perform or assist the District in performing the search. If reasonable suspicion exists and either (a) the student refuses to provide the District with access to their account to perform the search or (b) the circumstances are such that the search must be performed before the student is consulted, then the District may use its administrative access to force a change of the password to facilitate the access. The District may disable access to an account to prevent relevant information from being deleted from the account while a particular matter is being

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

reviewed. Absent extraordinary circumstances, parents/guardians will be notified that their child's device has been subject to a search and the outcome of that search.

Searches shall occur only under the direction of the Supervisor of Technology Operations or the Director of Information Technology and Cybersecurity in consultation with the student's principal and with the Superintendent's designee and/or legal counsel. The Information Technology and Cybersecurity Department will maintain a written record of District searches of individual student accounts, including, at a minimum, the following:

- the date and time the account was accessed,
- the name of the student whose account was accessed,
- the individual requesting the access,
- the reason that access was requested,
- the signature of the student in the event that consent was given for the access,
- the scope of the search,
- the results of the search,
- the person conducting the search.

In addition to periodically reviewing the written record of District searches of student accounts, and to the extent technologically practical, the Director of Information Technology and Cybersecurity will audit searches, no less than annually, to include the accounts that have been searched, the persons conducting the searches, and the date/time of the searches. The Director of Information Technology and Cybersecurity will report any significant findings to the Superintendent.

CAVEAT to District-Conducted Searches: Where the suspected violation of the school disciplinary code may in any way involve sexually explicit visual depictions of students or other minors (under 21), no search shall be performed by District personnel, and the matter will be referred to law enforcement for appropriate action.

D. Classroom Management and Supervision

Technology safeguards, including internet filtering, monitoring systems, and security controls, are important components of the District's student safety program. However, no technological solution can prevent all instances of misuse.

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

In accordance with Policy and Administrative Regulation 141 (K-12 Technology Use) as well as this Policy and Administrative Regulation, Employees are expected to exercise reasonable supervision of student technology use and to:

- monitor student use of District Technology Resources during instructional activities;
- promote responsible Digital Citizenship and appropriate online behavior;
- provide age-appropriate guidance regarding the safe, ethical, and educational use of technology;
- ensure technology use supports instructional objectives;
- encourage students to engage in non-digital learning experiences when technology is not necessary to accomplish instructional objectives;
- address inappropriate technology use promptly and report concerns as appropriate; and
- take reasonable steps to ensure students access approved educational resources during instructional activities.

E. Parent Portal

The District may provide parents and guardians with access to a Parent Portal or similar technology designed to promote student safety, responsible technology use, and family engagement.

The Parent Portal will enable parents and guardians to:

- review their student's District-issued device activity;
- monitor internet usage outside of school hours;
- temporarily pause or restrict access to District-issued devices outside the instructional day; and
- access resources supporting digital citizenship and online safety.

The Parent Portal supplements, but does not replace, District filtering, monitoring, supervision, and other safety measures. Access to student information through the portal shall be governed by FERPA and other applicable privacy laws. Parents and guardians are responsible for maintaining the confidentiality of their portal credentials.

F. No Expectation of Privacy

Students and other users of District Technology Resources should not expect that files or other information stored on the District's Network or other Technology Resources will be private as to the District. Privacy rights in connection with service providers will be

Lower Merion School District

ADMINISTRATIVE REGULATIONS

Policy No.: 142
Section: PROGRAMS
Title: K-12 TECHNOLOGY: SAFETY,
MONITORING AND PRIVACY
Date Adopted: 8/17/26

determined by the End User Licensing Agreement with that service provider. Some online educational service providers may log user information, such as IP Address. The District also has the ability to collect, track and store IP addresses to identify devices using and communicating over the District's network and other technology resources such as online services. The District reserves the right to utilize IP address information it obtains for troubleshooting and investigative purposes. Monitoring shall be conducted only for legitimate educational, operational, safety, security, or legal purposes and in accordance with District policy and applicable law.

IV. 2026-27 Implementation

For purposes of supporting the implementation of this Policy and Administrative Regulation, the attached **Addendum A** is provided as a plain-language, public-facing resource intended to further explain and clarify their provisions. **Addendum A** should be read in conjunction with the Policy and Administrative Regulation and is not intended to modify, expand, or supersede their requirements. In the event of any inconsistency or conflict, the language of the Policy and Administrative Regulation shall control.

Cross References:

- Board Policy and Admin. Reg. 114 (Individual Student Supports and Services)
- Board Policy and Admin. Reg. 235 (Student Rights and Responsibilities)
- Board Policy and Admin. Reg. 141 (K-12 Technology Use)