ATTACHMENT A

Administrative Regulation 142 (K-12 Technology: Safety, Monitoring and Privacy)

Implementation Summary – 2026-27

Purpose

This summary translates Administrative Regulation 142R into a plain-language description of how Lower Merion School District protects students, manages educational technology, safeguards information, and uses filtering, monitoring, classroom supervision, and family controls. It is intended to help students, families, staff, and community members understand the practices that operate alongside the Regulation.

What the District Protects

The District treats student safety, instructional quality, privacy, and cybersecurity as connected responsibilities. Administrative Regulation 142R establishes requirements for District Technology Resources, including networks, servers, telecommunications systems, District-issued devices, cloud storage, and District-provided web or cloud applications. Key components include:

- *Student privacy and personally identifiable information:* The District evaluates digital resources so that student data is collected, used, and shared only for legitimate educational purposes and consistent with applicable law, including Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA).
- *Information security:* The vendor review process assesses security features such as encryption, access controls, incident response, and breach notification procedures.
- *Online safety:* The District uses technology protections to restrict obscene material, pornography, child pornography, and other visual depictions that are harmful to minors, consistent with Children's Internet Protection Act (CIPA) requirements.
- *Appropriate instructional use:* Technology is expected to support meaningful learning, active engagement, collaboration, problem-solving, and other educational purposes.

How Educational Technology Is Approved

The District maintains a review process that extends beyond purchasing. A proposed digital product is evaluated for educational value, privacy, cybersecurity, operational feasibility, accessibility, cost, and long-term sustainability before approval. Every request identifies the educational or operational purpose, intended users and grade levels, devices and access methods, account creation and oversight, implementation requirements, funding source, expected cost, renewals, and whether the request creates a new vendor relationship.

Requestors identify what categories of information will be shared with the vendor, how accounts will be created and managed, whether administrative accounts are required, who will administer them, and whether access occurs on or off campus. The process is designed to disclose only the minimum information necessary for the educational purpose.

The review is cross-functional. Curriculum, Technology Services, Business Office staff, legal counsel, and instructional leaders evaluate proposals from their respective perspectives. Legal review considers privacy, data ownership, security, liability, and regulatory compliance. When

needed, the District may present vendors with a District-developed contractual addendum establishing privacy and data security protections.

Approved products are documented in the District's records, supporting ongoing management of vendors, licensing, renewals, duplicate tools, and ownership.

This approval process is designed to ensure that technology is selected because it advances teaching and learning and can be used responsibly and not simply because a product is popular, readily available, or inexpensive.

Data Privacy and Security Practices

Protecting student information is an ongoing responsibility. The District combines application review, contractual protections, information security practices, and lifecycle oversight to reduce unnecessary collection and use of student and staff information. Vendor privacy terms, terms of service, and data collection practices are reviewed as part of the application approval process. The District seeks additional contractual protections (described below) that prohibit vendors from selling, monetizing, or otherwise improperly disclosing personally identifiable student or staff information.

Vendors that will have access to District information are required to accept the District's standard contractual addendum. The addendum supplements the vendor's underlying agreement, privacy policy, terms and conditions, and other governing terms and establishes enforceable District requirements for the handling and protection of student, employee, and other District information.

The District's contractual protections include:

- *Limited Educational Use of Student Data.* Vendors may access and use personally identifiable student information only as necessary to provide the educational services contracted for by the District. Vendor employees, contractors, and other authorized individuals with access to District records must maintain the information confidentially, may not redisclose it without District authorization, and may use it only for the limited purpose of providing services to the District.
- *Restricted Access and Confidentiality.* Access to District records is limited to vendor employees and contractors who need the information to perform the contracted service, persons otherwise legally entitled to access it, or persons specifically authorized by the District. Individuals receiving access must themselves be subject to confidentiality and use restrictions consistent with the District's requirements. The vendor's contractual confidentiality and nondisclosure obligations continue beyond the term of the agreement.
- *Protection Extending Beyond Traditional Student Records.* Contractual protections apply to personally identifiable information in District records regardless of whether information might otherwise qualify as "directory information." The addendum also extends comparable protections to sensitive information that a vendor may encounter, including health information, employee and payroll information, financial information, employee evaluations

or investigations, immigration information, and other information designated by the District as sensitive data.

- *No Targeted Advertising or Marketing to Students.* Vendors may not engage in targeted advertising or marketing to District students and may not permit third parties to conduct targeted advertising or marketing through the vendor's programs, services, or platforms.
- *No Sale or Advertising-Related Disclosure of Student Information.* Vendors may not sell, transfer, or otherwise disclose personally identifiable information contained in District records to third-party advertising, marketing, or promotional companies.
- *District and User Control of Data.* The District remains the source and controller of student education records for purposes of responding to parent and eligible-student requests for access or amendment. Users also retain ownership and rights in the data and content they submit. A vendor may use user-generated content only for the limited purpose of performing its contractual obligations to the District.
- *Deletion and Secure Destruction.* At the District's request, vendors must delete District records maintained on their servers, securely destroy paper records, and certify to the District that the required deletion and destruction have occurred.
- *Cybersecurity Safeguards.* Vendors must undertake commercially reasonable measures to protect the availability, integrity, and confidentiality of District information. Contractual requirements include security practices consistent with reasonable industry standards, vulnerability assessment, monitoring for security breaches, current antivirus protections and security patches, virus scanning, and firewall and/or intrusion-prevention protections.
- *Data Backup and Recovery.* Vendors are required to maintain data-backup and restoration capabilities designed to protect District information from loss. The District's standard addendum establishes minimum backup expectations and makes the vendor financially responsible for certain direct costs resulting from a failure to meet those obligations.
- *Immediate Breach Notification and Response.* A vendor experiencing a breach or unauthorized disclosure of District information must immediately notify the District in writing and identify the extent of the incident. Vendors are responsible for legally required notifications to affected individuals and must cooperate with the District when the District determines additional notification is appropriate. The addendum also allocates specified notification costs to the vendor.
- *District Remedies Following a Data Breach.* The District retains the right to terminate an agreement immediately and without penalty following a breach or unauthorized disclosure of District information and to pursue other corrective action permitted by law.
- *Protection Against Unanticipated Changes in Vendor Practices.* Vendors must provide at least 30 days' advance notice of material changes to their privacy policies, terms and conditions, or other governing terms. The District may terminate the agreement without penalty when such changes are unacceptable.

- *Protection During a Sale, Merger, or Corporate Transaction.* A vendor must provide advance notice when a merger, acquisition, asset sale, restructuring, or similar transaction would involve the transfer of District student information. The District retains the ability to terminate the agreement and prevent the transfer of that information.
- *Restrictions on Subcontracting and Assignment.* Except for the specifically addressed corporate transactions, vendors may not assign contractual responsibilities or subcontract covered services without prior written consent, providing the District additional control over which entities may perform services involving District information.
- *Compliance with Student Privacy Laws.* Vendors must comply with applicable federal, state, and local requirements, expressly including FERPA and COPPA where applicable.
- *Digital Accessibility.* Vendor-provided websites, applications, online platforms, digital documents, multimedia, social media content, and other electronic communications must comply with WCAG 2.1 Level AA throughout the contract term. Vendors must conduct accessibility testing, provide certification upon request, and remediate identified deficiencies at their expense.

Taken together, these contractual requirements are intended to ensure that approval of an educational technology resource is not based solely on a vendor's representations or published privacy policy. Where applicable, the District establishes its own contractual requirements governing who may access District information, the purposes for which information may be used, how it must be secured, when it must be deleted, what happens following a breach or change in vendor practices, and the District's continuing control over student and other sensitive information.

Filtering, Internet Safety, and Classroom Controls

The District uses a layered model of protection designed to preserve access to legitimate instructional resources while limiting unsafe, inappropriate, or non-instructional content. These strategies include, but are not limited to:

- The District recently evaluated multiple filtering and device-management platforms and selected Securly because it provided a strong combination of student protection, instructional flexibility, classroom management, and parent controls.
- SSL decryption is enabled to help identify and block attempts to bypass internet filters through proxy websites or similar evasion tools.
- Filtering has been expanded to block categories of sites that are not related to curriculum or instruction, including social media platforms, streaming entertainment services, and artificial intelligence summary sites that may encourage students to bypass the learning process.
- Access to publicly available Google Sites is restricted to Google Sites created and managed by LMSD teachers for instructional purposes.
- Teachers have classroom-management tools that can direct students to specific instructional websites, create class-specific allow and block lists, limit browser tabs during instruction, and monitor student device activity to support assigned learning tasks.

No filtering software is completely secure or effective. A website or material that is not blocked is not necessarily appropriate. Technology protections are one part of a broader student-safety approach that includes adult supervision, digital citizenship, and clear expectations for responsible use.

Family Oversight Outside School

The Regulation authorizes a Parent Portal to support student safety, responsible technology use, and family engagement. The District's implementation provides families with additional visibility and control over District-issued devices outside instructional hours.

- Parents/guardians may review internet activity associated with their student's District-issued device.
- Outside school hours, families may apply stricter filtering, block specific websites or categories, establish schedules for device use, or temporarily pause access to District-issued devices.
- Families may see usage during the school day, but the family controls do not give parents/guardians control over District-issued devices during the instructional day.

Teacher and Staff Responsibilities

Technology safeguards do not replace active supervision. During instructional activities, employees are expected to exercise reasonable supervision and help students use technology safely, ethically, and for educational purposes. With support from administration, teachers are responsible for:

- Monitoring student use of District Technology Resources during instructional activities.
- Promoting responsible Digital Citizenship and appropriate online behavior.
- Ensuring technology use supports instructional objectives and encourage non-digital learning when technology is not necessary.
- Addressing inappropriate technology use promptly and report concerns as appropriate.

Monitoring, Searches, and Accountability

Administrative Regulation 142R distinguishes between routine technology monitoring and targeted searches when there is reasonable suspicion of a policy, school-rule, or legal violation. Monitoring and searches are subject to defined purposes, authorization, scope, and documentation requirements.

- *General monitoring:* The District may periodically review files and communications stored or shared on District Technology Resources to identify inappropriate, threatening, harassing, copyrighted, or security-related material. Files may be removed or quarantined when permitted by law or District policy.
- *Reasonable-suspicion searches:* When authorized administrators have reasonable grounds to believe a student has violated law, school rules, or District policy, the District may search relevant District technology accounts and resources. The scope of the search must be reasonably related to the suspected violation.

- *Authorization and consultation:* Searches are directed by designated Technology leadership in consultation with the student's principal and the Superintendent's designee and/or legal counsel, as required by the Regulation.

No Expectation of Privacy on District Technology

Students and other users should not expect that files or information stored on the District Network or other District Technology Resources will be private as to the District. Service-provider privacy practices are also governed by applicable end-user agreements and other contractual terms.

The District may collect, track, and store IP addresses to identify devices communicating over District networks or online services and may use IP address information for troubleshooting and investigative purposes.

Monitoring is conducted only for legitimate educational, operational, safety, security, or legal purposes and in accordance with District policy and applicable law.

Ongoing Review and Improvement

The District continually reviews its filtering, monitoring, application approvals, and related technology systems in response to emerging technologies, evolving online risks, significant vendor changes, security incidents, privacy revisions, and changing instructional needs. The goal is to maintain a safe, productive learning environment while preserving meaningful access to technology that supports teaching and learning.

Related District authorities: Board Policy and Administrative Regulation 142; Administrative Regulation 141 (K-12 Technology Use); Board Policy and Administrative Regulation 114 (Individual Student Supports and Services); and Board Policy and Administrative Regulation 235 (Student Rights and Responsibilities).