REVISION

CYBERSECURITY AND DATA PRIVACY

Original Adopted Date: 06/21/2022 **| Last Revised Date**: N/A

The Board of Education recognizes the responsibility to adopt appropriate administrative, technical, and physical safeguards and controls to protect and maintain the confidentiality, integrity and availability of its data, data systems, and information technology resources.

The purpose of this policy is to ensure the implementation of industry security standards and best practices to protect sensitive data, student records, direct/indirect identifiers, and the ~~D~~district's technology infrastructure.

It is the responsibility of Lodi Unified School District:

- To comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information;
- To maintain a comprehensive Cybersecurity and Data Privacy Program designed to satisfy its statutory and regulatory obligations, enable, and assure core services, and fully support the ~~D~~district's goals;
- To protect personally identifiable information (PII), and sensitive and confidential information from unauthorized use or disclosure;
- To address the adherence of its vendors to federal, state, and California Education Code requirements in vendor agreements;
- To train its users to share a measure of responsibility for protecting Lodi Unified School District student data and data systems;
- To identify its required cybersecurity and data privacy responsibilities and goals, integrate them into relevant processes, and commit the appropriate resources towards the implementation of such goals; and
- To communicate its required cybersecurity and data privacy responsibilities and goals, and the consequences of non-compliance, to its users.

Scope

The policy applies to all Lodi Unified School District employees, interns, volunteers ("Users"), and third-party contractors who receive or have access to Lodi Unified School District data, network and/or online systems.

This policy encompasses all systems, automated and manual, including systems managed or hosted by third parties on behalf of the ~~D~~district, and addresses all information, regardless of the form or format, which is created or used in support of the activities of the district.

Security Standards

Lodi Unified School District utilizes the Center for Internet Security (CIS) Critical Security Controls® as the standard for the ~~D~~district's Cybersecurity and Data Privacy Program to ensure the highest standards of cybersecurity practices throughout the ~~D~~district. A series of procedures based on each CIS Security Control

will be developed in partnership with the Center for Internet Security, San Joaquín County of Education, and other resources.

Data Privacy

a. State and federal laws, such as the Family Educational Rights Privacy Act (FERPA), California Education Code 49073.1, and others, establish baseline parameters for what is permissible when sharing student PII.
b. Data protected by law must only be used in accordance with Education Code policies to ensure it is protected from unauthorized use and/or disclosure.
c. Lodi Unified School District has established a Technology Acquisition Process (TAP) to manage its use and sharing of data protected by law. The TAP review team, together with program administrators, determine whether a proposed use of PII would benefit students and curriculum programs, and ensure that PII is not included in public reports or other public documents, or otherwise publicly disclosed.
d. No student PII data shall be shared with third parties, which includes free online services without a California Student Data Privacy written agreement that complies with state and federal laws and regulations or signed parental consent. No student data will be provided to third parties unless it is permitted by state and federal laws and regulations. Third-party contracts must include data safeguards and provisions required by state and federal laws and regulations.
e. Contracts with third parties that will receive or have access to PII must outline how the contractor will ensure the confidentiality of data is maintained in accordance with state and federal laws and regulations and this policy.
f. It is Lodi Unified School District's policy to provide all protections afforded to parents and persons in parental relationships, or students where applicable, as required under FERPA, the Individuals with Disabilities Education Act, and the federal regulations implementing such statutes. Therefore, Lodi Unified School ~~D~~district shall ensure that its contracts require that the confidentiality of student data be maintained in accordance with federal and state law and this policy.

Incident Response and Notification

The Superintendent or designee will respond to cybersecurity and data privacy incidents in accordance with ~~D~~district Cybersecurity and Data Breach Notification procedures and Incident Education Code regulations. The ~~D~~district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any cybersecurity attack or other cybersecurity incident.

Acceptable Use

Lodi Unified School District Technology Services department is obligated to conserve and protect ~~D~~district resources for the benefit of the public interest; however, the responsibility and accountability for the appropriate use of ~~D~~district resources rests with the individual who uses the resource or who authorizes such use. Noncompliance with board policy may result in disciplinary action consistent with ~~D~~district policies and/or, if appropriate, termination of contracts and services with the ~~D~~district. Violations of the law may result in criminal prosecution and/or disciplinary action by the ~~D~~district.

Access to ~~D~~district technology resources, including the internet, shall be made available to users for instructional and administrative purposes and in accordance with federal and state laws, ~~D~~district policies and job functions.

Access privileges will be granted in accordance with the user's job responsibilities and will be limited only to those necessary to accomplish assigned tasks by job functions (i.e., least privilege). All ~~D~~district user

accounts will utilize a form of Multi-factor Authentication, also known as MFA or 2FA. Accounts will be removed, and access will be disabled, for all those who have left the ~~D~~district unless otherwise authorized by the Superintendent or designee.

Employees will communicate via e-mail, on district authorized equipment through their assigned lodiusd.net/org or other ~~D~~district accounts as assigned. District or student data will not be sent to or forwarded to an employee's personal email account.

Only ~~D~~district authorized equipment shall be permitted to be connected to the ~~D~~district's internal networks. A guest wireless network may be made available for guest devices. Superintendent's Cabinet approval is required for guest wireless access to non-~~D~~district owned devices. Guest access is governed by all ~~D~~district policies and acceptable agreements.

Security Awareness and Training

All users with access to ~~D~~district data, technology resources, and data systems must annually complete the cybersecurity and data privacy training offered by the ~~D~~district. In addition, the ~~D~~district will conduct ongoing cybersecurity awareness campaigns and may require further training to promote continued awareness and education of cybersecurity risks.

Policy Adopted: 06/21/2022
Revised: N/A