Student Data Privacy and Security

Section A - Introduction

Technologies used in the school district shall further the objectives of the school district's educational program and/or support efficient school district operations. The school district and/or vendors under its control may need to collect and maintain data that personally identifies students in order to use certain technologies for the benefit of student learning or school district operations.

Federal and state laws govern the protection of student data. The sale, rental, lease, or trading of any such data by the school district is prohibited. Protecting such data is important for legal compliance, school district operations, and the trust of school district stakeholders, including parents, students, and staff.

Section B - Definitions

Covered information: Personally identifiable information (PII) or information linked to PII in any media or format that is not publicly available and is any of the following: (1) created by or provided to an operator by a student or the student's parent/guardian in the course of the student's or parent/guardian's use of the operator's site, service, or application; (2) created by or provided to an operator by an employee or agent of the school district; or (3) gathered by an operator through the operation of its site, service, or application.

Operators: Entities that operate internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes.

Breach: The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or the school district.

Section C - Operator Contracts

The Superintendent or designee is authorized to enter into contracts with operators that do not require separate Board approval. Contracts between the Board and operators shall be entered into in accordance with Board Policy 4200 and posted to the school district's website as required by state law.

Section D - Security Standards

The Superintendent or designee shall ensure that the school district implements and maintains reasonable security procedures and practices that meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure. In the event the school district receives notice from an operator of a breach or has determined a breach has occurred, the Superintendent or designee shall ensure that the school district provides any breach notifications required by state law.

Section E - Notifications

The Superintendent or designee shall provide annual notice to parents/guardians regarding PII information shared with approved operators.

Approved: TBD