Students

Administrative Procedure – Use of Educational Technologies; Student Data Privacy and Security

Use this procedure to establish a process for evaluating the use of educational technologies for student learning and/or District operations, and to facilitate compliance with the Student Online Personal Protection Act (SOPPA), amended by P.A. 101-516, eff. 7-1-21.

Definitions (105 ILCS 85/5, amended by P.A. 101-516, eff. 7-1-21)

Covered information means 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 District; or (3) gathered by an operator through the operation of its site, service, or application.

Operators are entities (such as educational technology vendors) that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes.

K-12 school purposes means purposes that are directed by, or that customarily take place at the direction of, a teacher, school, or school district; aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents; or are otherwise for the use and benefit of a school.

Breach means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of covered information maintained by an operator or the District.

Parent means a person who is the natural parent of the student or other person who has the primary responsibility for the care and upbringing of the student.

Educational Technologies Evaluation and SOPPA Implementation

Actor	Action
Superintendent or Designee or Privacy Officer	1. Establishes an Educational Technology Committee (Ed Tech Committee) to operate as a Superintendent committee for the purposes of: (1) evaluating the use of specific online applications and other educational technologies within the District, (2) establishing a list of applications or other services approved for use within the District, and (3) developing a process for the approval of online sites, applications, or services not already approved for District use which staff members may wish to use. See 2:150-AP, *Superintendent Committees*. Consider including: Head of Information Technology (IT) Other district-level administrators, such as Curriculum Director, Student Services Director, Business Manager Building Principals Teachers **Note:** This procedure establishes an administrative committee.

	The administrative committee centralizes the local decision-making process regarding the use of educational technologies in a district, which in turn should help districts comply with the provisions of SOPPA governing the use of covered information by operators, contractual requirements, and security standards. 2. Informs the School Board of the Ed Tech Committee's progress. 3. Makes recommendations to the Board about operator contracts, as needed and in alignment with Board policy 7:345, *Use of Educational Technologies; Student Data Privacy and Security*. 4. Designates which District employee(s) are authorized to enter into written agreements with operators when prior board approval of the contract is not otherwise required by Board policy 4:60, *Purchases and Contracts*, and list them below: _____ _____ Title Title _____ _____ Title Title 5. Assigns the following activities to the Head of IT and the Records Custodian: a. Develop and maintain a protocol to manage parent requests for copies (electronic and paper) of students' covered information. b. Develop and maintain a protocol to manage parent requests for corrections to factual inaccuracies contained in a student's covered information. c. Develop and maintain a protocol to manage parent requests for deletion of a student's covered information maintained by an operator. 6. Ensures that the parent of any student whose covered information was involved in a breach is provided with a breach notification letter no later than 30 calendar days after the District determines a breach has occurred or has been notified by an operator of a breach, unless an appropriate law enforcement agency has requested in writing that the District not provide breach notifications because doing so would interfere with a criminal investigation. See 7:345-AP, E3, *Parent Notification Letter for Student Data Breach*. 7. As appropriate, notifies the District's liability carrier of any third party claims made against the District regarding a data breach. 8. Consults with the Board Attorney for guidance as needed to ensure the District complies with the provisions of SOPPA.
Head of IT or Privacy Officer	1. Implements and maintains reasonable cybersecurity

practices to protect covered information, such as technical, administrative, and physical safeguards that are consistent with any guidance from the Ill. State Board of Education (ISBE) and 6:235-AP1, Acceptable use of the District's Electronic Networks. Coordinates with the Superintendent to implement any staff training on such practices. Coordinates with the Business Manager regarding any recommendations for purchases of equipment or software related to cybersecurity.

2. Creates, maintains, and regularly updates an internal inventory of all Internet websites, online services, online applications, and mobile applications that are being used in the District for K-12 purposes. Note: The inventory does not need to include general audience websites, online services, online applications, or mobile applications, even if login credentials are required to access the general audience sites, services, or applications.

   The inventory list should include the following, and any other information deemed pertinent:
   a. Name of Operator
   b. Contract term and expiration/renewal date
   c. K-12 purpose for which the online service, application, etc. is being used (e.g., curriculum content area and grade level(s))
   d. A listing of the data elements of covered information that the District collects, maintains, or discloses to the operator.
   e. A layperson explanation of the data elements listed for each operator including how the district uses the information, to whom or what entities it discloses the information, and for what purpose(s) the information is used.
3. Ensures the following information is posted on the District's website and updated (if needed) by Jan. 31 and July 31 each year (105 ILCS 85/27(a), added by P.A. 101-516, eff. 7-1-21) (See 7:345-AP, E1, Student Covered Information Reporting Form):
   a. A list of operators with which the District has written contracts. 105 ILCS 85/27(a)(2).
   b. Copies of the District's written contracts with operators, with redactions as permitted by State law and mutually agreed upon between the District and operators. 105 ILCS 85/27(a)(2).
   c. Business address of each operator. 105 ILCS 85/27(a)(2).
   d. For each operator, a list of any subcontractors to whom covered information may be disclosed or a link to a page on the operator's website that clearly lists that information. 105 ILCS 85/27(a)(3).
   e. An explanation that is clear and understandable by a layperson, of the following (105 ILCS 85/27(a)(1)):
      i. The data elements of covered information that the District collects, maintains, or discloses to any person, entity, third party, or governmental agency.
      ii. To whom or to what entities the covered information is disclosed.
      iii. How the covered information is used.
      iv. The purpose of the disclosure of the covered information.
   f. For breaches involving 10% or more the District's enrolled students, a list of any breaches of covered information maintained by the District or by an operator that includes the following information (105 ILCS 85/27(a)(5), added by P.A. 101-516, eff. 7-1-21):
      i. The number of students whose covered information was involved in the breach, unless the breach involves the personal information of students, as defined by the Personal Information Protection Act, 815 ILCS 530/10. Personal information means either:
      1. A student's first name or first initial and last name in

	combination with any one or more of his or her (a) social security number, (b) driver's license number or State ID card number, (c) financial account information (with any required security codes or passwords), (d) medical information, (e) health insurance information, and/or (f) unique biometric data or other unique physical or digital representation of biometric data, when either the name or data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired through the breach of security; or 2. A student's username or email address, in combination with a password or security question and answer that would permit access to an online account, when either the username or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted, but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security. g. A written description of the procedures a parent may use to carry out their rights to: (1) inspect and review his/her child's covered information; (2) request electronic or paper copies of his/her child's covered information and (3) request corrections to his/her child's inaccurate covered information under SOPPA. 105 ILCS 85/27(4), added by P.A. 101-516, eff. 7-1-21. 4. Posts on the District's website any new operator contracts within 10 business days of the District entering into the contract, along with the information required in items 3.a. through 3.e. listed immediately above. 105 ILCS 85/27(c), added by P.A. 101-516, eff. 7-1-21. 5. Promptly notifies the Superintendent of any breach of covered information or other personal information of students so that appropriate notices can be provided.
Business Manager or Privacy Officer	1. Assists Head of IT in creating, maintaining, and updating the internal inventory list referenced in the row above. 2. Reviews operator contracts (including electronic agreements, click wrap agreements, or other terms and conditions a user must agree to before using the product or service) before approval to ensure they contain the provisions required by SOPPA (this can also be accomplished through the Business Manager's participation in the Committee described above). The following provisions are required for contracts entered into, renewed, or amended on or after 7-1-21, if the operator is seeking in any manner any covered information from the District (105 ILCS 85/15(4), added by P.A. 101-516, eff. 7-1-21): a. A listing of the categories or types of covered information to be provided to the operator. b. A statement of the product or service being provided to the District by the operator. c. A statement that, pursuant to the federal Family Educational Rights and Privacy Act of 1974 (FERPA), the operator (1) is acting as a school official with a legitimate educational interest, (2) is performing an institutional service or function for which the District would otherwise use employees, (3) is under the direct control of the District, with respect to the use and maintenance of covered information, (4) is using the covered information only for an authorized purpose and (5) may not re-disclose covered information to third parties without the District's permission or pursuant to a court order. d. A description of how, if a breach is attributed to the operator, any costs and expenses incurred by the District in investigating and remediating the breach will be allocated between the operator and District. The costs and expenses may include, but are not limited to: (1) providing notification

	to parent of those students whose covered information was compromised and to regulatory agencies or other entities as required by law or contract, (2) providing credit monitoring to those students whose covered information was exposed in a manner during the breach that a reasonable person would believe that it could impact his or her credit or financial security, (3) legal fees, audit costs, fines, and any other fees or damages imposed against the school as a result of the security breach; and (4) providing any other notifications or fulfilling any other requirements adopted by the Ill. State Board of Education or of any other State or federal laws e. A statement that the operator must delete or transfer to the school all covered information if the information is no longer needed for the purposes of the written agreement and to specify the time period in which the information must be deleted or transferred once the operator is made aware that the information is no longer needed for the purposes of the written agreement. f. If the District maintains a website, a statement that the District must publish the written agreement on the District's website. If the school does not maintain a website, a statement that the District will make the written agreement available for inspection by the general public at its administrative office. 3. As permitted by State law, obtains the operator's agreement regarding what provisions, if any, of the contract will be redacted in the copy that is posted on the District's website. Items 2.a, 2.b, and 2.c in the list immediately above may NOT be redacted in the posted copy. 4. Ensures that the District also has written agreements in place that include the provisions listed in #2 above whenever it shares, transfers, discloses, or provides access to a student's covered information to an entity or individual, other than the student's parent, school personnel, Board members, or ISBE, unless the disclosure or transfer is (1) required by court or State or federal law or (2) to ensure legal or regulatory compliance. 105 ILCS 85/26(2), added by P.A. 101-516, eff. 7-1-21. 5. With the authorization of the Superintendent, consults with the Board Attorney as needed for contract review. 6. Provides a copy of all operator contracts to the Head of IT for posting on the District's website.
Head of IT and Records Custodian or Privacy Officer	1. Develops and maintains a protocol to manage parent requests to inspect and review their child's covered information, whether it is maintained by the District, ISBE, or an operator. 105 ILCS 85/33(c)(1), added by P.A. 101-516, eff. 7-1-21. If the covered information is a school student record, then follow the procedures and timelines for responding to student record requests in 7:340-AP1, School Student Records. 2. Develops and maintains a protocol to manage parent requests for copies (electronic and paper) of students' covered information. Align the protocol with the following requirements (105 ILCS 85/33(c)(2), added by P.A. 101-516, eff. 7-1-21): a. If the parent requests an electronic copy of the student's covered information, the District must provide an electronic copy of the information, unless the District does not maintain it in an electronic format and reproducing the information in an electronic format would be unduly burdensome to the District. b. If the parent requests a paper copy of the student's covered information, the District may charge the parent the reasonable cost of copying in an amount not to exceed the amount fixed in a schedule adopted by ISBE. However, the parent may not be denied a copy of the information due to the parent's inability to pay the cost of copying. c. The protocol must be consistent with any regulations

	issued by ISBE. d. If the covered information is a school student record, then follow the procedures and timelines for responding to student record requests in 7:340-AP1, School Student Records. 3. Develops and maintains a protocol to manage parent requests for corrections to factual inaccuracies contained in a student's covered information. Align the protocol with the following requirements (105 ILCS 85/33(c)(3), added by P.A. 101-516, eff. 7-1-21): a. The District must determine whether the factual inaccuracy exists. b. If the District determines that a factual inaccuracy exists, and the District maintains or possesses the covered information, it must correct the inaccuracy and confirm the same with the parent within 90 calendar days after receiving the parent's request. c. If the District determines that a factual inaccuracy exists and an operator or ISBE maintains or possesses the information, the District must notify the operator or ISBE of the factual inaccuracy and correction to be made. The operator or ISBE must confirm the correction with the District within 90 calendar days after it receives the District's notice. The District must then confirm the correction with the parent within 10 business days after receiving confirmation of the correction from the operator or ISBE. d. If the covered information is a school student record, and the parent requests a hearing to challenge the accuracy of the record(s), follow the procedures and timelines in 7:340-AP1, School Student Records. 4. Develop and maintain a protocol to manage parent requests for deletion of a student's covered information maintained by an operator. Align the protocol with the following requirements: a. Deny the request if granting it would result in a violation of the Ill. School Student Records Act or other records laws, such as the deletion of a school student record (temporary or permanent) that the District is required by law to maintain for a certain period of time. 105 ILCS 85/27(g), added by P.A. 101-516, eff. 7-1-21. b. Consider denying the request if granting it would effectively result in the student being unable to participate in all or a portion of the District's curriculum through the site, service, or application being used.
Building Principal(s) or Privacy Officer	1. Ensures that parents are provided with 7:345-AP, E2, Notice to Parents About Educational Technology Vendors, at the beginning of each school year through distribution of school handbooks or other means generally used by the building to provide such notices to parents. 105 ILCS 85/28(e), added by P.A. 101-516, eff. 7-1-21. 2. Promptly communicates any parent requests for copies of, corrections to, or deletion of students' covered information to the Records Custodian and Head of IT.
Staff Members	1. Participate in any District-required trainings on the privacy and security of student data. 2. Refrain from using any new online sites, services, or applications that collect any student data or covered information that have not be pre-approved for use by the District. 3. Be familiar with and abide by policy 6:235, Access to Electronic Networks, and 6:235-AP1, Acceptable Use of the District's Electronic Networks.

K-12 Data Privacy and Cybersecurity Resources:

www.studentprivacy.ed.gov/

www.ltcillinois.org/resources/dataprivacy/

www.ferpasherpa.org/resources/

www.k12cybersecure.com/resources/

www.cosn.org/ProtectingPrivacy

Attai, Linnette. Student Data Privacy: Building a School Compliance Program. (Rowman & Littlefield, 2018).