WITHDRAWN

20-1118-PO1

November 18, 2020

ADOPT A NEW STUDENT ONLINE PERSONAL PROTECTION ACT (SOPPA) POLICY

THE CHIEF EXECUTIVE OFFICER RECOMMENDS THE FOLLOWING:
That the Board of Education ("Board") adopt a new Student Online Personal Protection Act (SOPPA) Policy effective July 1, 2021. The policy was posted online for public comment from October 2, 2020 to November 2, 2020.

PURPOSE: The state SOPPA law requires school districts to adopt a policy regarding the use of education technology products or applications. SOPPA is intended to ensure that student data will be protected when it is collected by educational technology companies and that the data may be used for beneficial purposes such as providing learning and innovative educational technologies. SOPPA requires: that school districts only use educational technologies that meet the following criteria: have been approved under this policy; all agreements between the Board and the provider are posted on district's website, and all of the data elements are listed on the district's website regardless if the Board pays for the tools or they are provided free of charge.

POLICY TEXT:

I. **SCOPE OF THE POLICY**: This policy outlines how Chicago Public Schools will comply with its responsibilities under SOPPA. This policy also provides how employees are authorized to use educational technology products or applications and which employees can enter into written agreements supporting or authorizing their use.

II. **DEFINITIONS:**

a. **Authorized Software** refers to any unique application, service, tool, program, platform, mobile application, product, electronic, or online tool, including free or complimentary software product or tool, that has been reviewed and approved for use on the CPS Network. These tools can be found on the Board's Authorized Software Student facing site.
b. **Breach** means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or school.
c. **Covered information** means personally identifiable information or material or information that is linked to personally identifiable information or material 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 in the course of the student's or parent's use of the operator's site, service, or application for pre-K through 12 school purposes.
    2. Created by or provided to an operator by an employee or agent of a school or school district for pre-K through 12 school purposes.
    3. Gathered by an operator through the operation of its site, service, or application for pre-K through 12 school purposes and personally identifies a student, including, but not limited to, the information in the student's educational record or electronic mail, first and last name, home address, telephone number, electronic mail address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, a social security number, biometric information, disabilities, socioeconomic information, food

purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

d. **Department/School Management** refers to the supervisor, manager, director, officer, principal, Network Chief, or other employees of the Board designated by their department or office or school to implement policy compliance requirements.
e. **Educational Technology** means educational software, electronic or online tools used by schools to improve student engagement, knowledge retention, individual learning or collaboration.
f. **Pre-K through 12 school purposes** refers to purposes that are directed by or that customarily take place at the direction of a school, teacher, 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 the school.
g. **Operator** refers to the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for pre-K through 12 school purposes and was designed and marketed for pre-K through 12 school purposes.
h. **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.
i. **Personally Identifiable Information (PII)** refers to sensitive data and information that must be protected against unwarranted disclosure such as student information, private employee information and protected health information that can adversely affect the privacy or welfare of an individual.
j. **Prohibited Software** refers to any software product or tool that is listed as 'prohibited for use' on the CPS Network. Prohibited software is identified after careful consideration and consensus amongst multiple departments that this technology has no place for Chicago Public Schools. The complete list of prohibited technology platforms is located on the district's AUP Guidance website: https://www.cps.edu/AcceptableUsePolicy/Pages/aup.aspx.
k. **Targeted advertising** means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or covered information. The term does not include advertising to a student at an online location-based upon that student's current visit to that location or in response to that student's request for information or feedback, without the retention of that student's online activities or requests over time for the purpose of targeting subsequent ads.

III. OPERATOR REQUIREMENTS:

Prior to entering into a written agreement with the district, operators must meet these minimum operator requirements.

a. Operators must agree to the following:
    1. Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

2. Publicly disclose material information about its collection, use, and disclosure of covered information with a privacy policy.
3. Limitations on a student's covered information.
    a) A student's covered information shall be collected only for pre-K through 12 school purposes and not further processed in a manner that is incompatible with those purposes.
    b) A student's covered information shall only be adequate, relevant, and limited to what is necessary in relation to the pre-K through 12 school purposes for which it is processed.
4. Notify the school of any breach of the students' covered information no later than 30 calendar days after the determination that a breach has occurred.

b. Operators are prohibited from:
    1. Engaging in targeted activities.
    2. Using information including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student.
    3. Selling or renting a student's information.
    4. Disclosing covered information, except for circumstances allowable under the SOPPA policy.

IV. REQUIREMENTS FOR APPROVING AUTHORIZED SOFTWARE:

a. Department/School Management may initiate an approval request for authorized software to meet an educational or operational need. The request will go through the following onboarding process.
    1. Initial Screening - The CEO or designee will create a minimum standard for software to be authorized (educational purpose and IT security).
    2. The onboarding process requires the reviews of the software by the following Departments:
    3. Education Technology - a further review of Ed-Tech Operations to determine if an education technology software meets the educational needs and requirements to be onboarded.
        a) Libraries and Instructional Technology
        b) Information Technology Services (ITS)
            (1) Information Security - Information Security will validate the operator has implemented and maintains reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.
            (2) Enterprise Architecture - How does the application fit in the current CPS environment.
            (3) Information Technology Infrastructure - Review operators for any ITS infrastructure requirements.
            (4) Project Management Office, Change Management and Training - to determine the steps required to implement the solution
        c) Law - Operators must agree to a contract that conforms with this policy and with SOPPA.
        d) Procurement - Create operator/sponsorship in CPS vendor database.
        e) Risk - Review operator's background check and insurance policy.

b. The Chief Educational Officer, Chief Procurement Officer, General Counsel, or their respective designee are the only school employees who may enter into a written agreement with operators. Any agreement or contract entered into by employees other than those listed above is in violation of SOPPA is void and unenforceable as against public policy.
c. All operators must have an agreement with the district posted on the public-facing district website, listing student data being transferred and all other information required by SOPPA before the software can be used in the district. If a program or platform is identified that does not have an agreement posted, that software use will be discontinued immediately and not reinstated until brought into compliance with an agreement posted including data field in use.

V. AUTHORIZED SOFTWARE:

a. Department/School Management or designee has the authority to select from a comprehensive list of authorized software.
b. Department/School Management may seek approval through the operator onboarding process to request an addition to the comprehensive list of authorized software.
c. No employee may use prohibited software.

VI. RESPONSIBILITIES FOR USING AUTHORIZED SOFTWARE:

a. School Use Procedures
    1. The principal must ensure teachers and staff are using authorized software.
    2. Principals may request approval for authorized software as noted in Section V of this policy.
b. Teacher and Staff Responsibilities
    1. Teachers and staff must receive approval from the principal prior to using authorized software.
    2. Teachers and staff must inform parents of the purpose of using the authorized software and if necessary obtain consent for use of authorized software.
c. Parent and Student Rights
    1. Parents have the right to Inspect and review the student's covered information, request from a school a paper or electronic copy
    of the student's covered information, and request corrections of factual inaccuracies contained in the student's covered information.
    2. Parents have the right to know which authorized software are being used in the classroom and to consent to the use of authorized software
    3. Parents have the right to be notified by the school or school district of a breach by an operator.

VII. WEBSITE POSTING:

The district will maintain and post the following on its website:

a. All data elements that the school district collects, maintains or discloses to any person, entity, or third party, or governmental agency used will be posted on the school's website. The post on the website must explain how the school district uses, to whom or what entities it discloses, and for what purposes it discloses the data elements/covered information.

b. All written agreements with operators involving SOPPA must be posted on the school district's website before the software can be used in the district.
c. A list of the operators that the school has written agreements with, including the copy of the agreement, the business address of each operator, whether the operator uses any subcontractors, and if so, a list of any subcontractors to whom covered information is being disclosed or a link to the operator's website where a list of these subcontractors is provided.

VIII. AUTHORIZATION TO ISSUE PROCEDURES AND GUIDELINES

The CEO or designee is authorized to establish guidelines as necessary to effectively implement the requirements of this policy, including when to revoke or review authorized software and how parents access their rights.

IX. ENFORCEMENT

Violations of this policy or any guidelines issued pursuant to or in relation to this policy are prohibited. Employees who commit violations may be subject to discipline. Operators who commit violations may result in their products or tools becoming prohibited.

LEGAL REFERENCES: Student Online Personal Protection Act, 105 ILCS 85/1.

Approved for Consideration:

DocuSigned by:
Phillip DiBartolo
1189156BA4E147B...

Phillip DiBartolo
Chief Information Officer

Approved:

DocuSigned by:
Janice K. Jackson
CD1308C15BA8459...

Janice K. Jackson
Chief Executive Officer

Approved for Consideration:

DocuSigned by:
LaTanya McDade
396384628F8A43A...

LaTanya D. McDade
Chief Education Officer

Approved as to Legal Form: DS KF

DocuSigned by:
Joseph T. Moriarty
571EC59C33144C5...

Joseph T. Moriarty
General Counsel