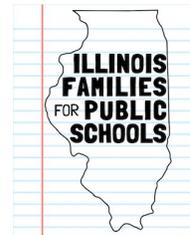


Illinois Families for Public Schools
332 S Michigan Ave
Lower Level Suite i252
Chicago IL 60604



November 2, 2020

Chicago Board of Education
1 N Dearborn ST, Suite 950
Chicago IL 60602

To the Chicago Board of Education:

Re: Draft policy on Student Online Personal Protection to be voted on at the November 18, 2020 meeting of the Chicago Board of Education

We are pleased to see that Chicago Public Schools have drafted a policy that covers more than the minimum requirements for a school district's written policy under PA-101-516.

There are several additional aspects of complying with the new requirements of PA-101-516 that we think would benefit students, parents and school personnel to have addressed explicitly in this policy. (For clarity, recommended wording changes are underlined or crossed out in the blue text sections below.)

Replace *vendor* with *operator*

PA-101-516 applies to any entity providing software to the district for PreK through 12 purposes whether or not the district will pay them for that software. In subitems IV(a)3b, IV(a)3e, and V(b), the proposed policy uses the term *vendor*, whereas those subitems should clearly apply to *all* operators, not just vendors. We recommend that all of those uses of *vendor* be replaced with *operator*.

In addition, subitem IV(a)3d should be rewritten as follows:

Procurement - Create vendor/sponsorship in CPS vendor database [for any operator that will be a vendor.](#)

Define *sell or rent*

We recommend the addition of a definition for *sell or rent* to be added to Section II. It is our position that the Illinois General Assembly, in passing both the original version of SOPPA and the amendment of SOPPA, intended to prevent operators from profiting off their access to student data that schools and students disclose to them. In order to clarify that operators shall never provide nor provide access to covered information to any third-party in exchange for a monetary or other consideration, we urge the district to clarify that the phrase *sell or rent* is defined in Section II as follows:

[Sell or rent refers to providing covered information to any third-party in exchange for a monetary or other consideration, regardless of whether that exchange is termed an act of selling, renting, leasing, licensing, or trading.](#)

Define *software* and replace some uses of *operator* with *software*

Although *authorized software* and *prohibited software* are included in Section II, we recommend the addition of a general definition for *software* as follows:

[Software refers to any computer software whether it is an application, service, tool, program, platform, Internet website or mobile application including free or complimentary software.](#)

Then we recommend that items V(a-c) be rewritten as such:

V. AUTHORIZED SOFTWARE:

- a. Department/School Management or designee has the authority to select software ~~an operator~~ from a comprehensive list of authorized software.
- b. Department/School Management that seeks to use software ~~an operator~~, not on this list must submit a request for approval through the software ~~vendor~~ onboarding process.
- c. No employee may use prohibited software.

For the sake of clarity, we recommend the following three edits as well in subitems IV(a)1-3:

1. Initial Screening - The CEO or designee will create a minimum standard for ~~products~~ software to be considered (educational purpose and IT security).
2. The onboarding process requires the reviews of the ~~solution~~ software by the following Departments:
3. Education Technology - a further review of Ed-Tech Operations to determine if ~~an education technology product~~ the software meets the educational needs and requirements to be onboarded.

Data deletion duties of schools and operators

PA-101-516 Sec 15.2 states that operators have the duty to:

"[d]elete, within a reasonable time period, a student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent consents to the maintenance of the covered information."

In addition, under Sec 27(g), schools have the duty to fulfill requests from parents to have their children's covered information deleted by communicating those requests to operators:

"A school shall make a request, pursuant to paragraph (2) of Section 15, to an operator to delete covered information on behalf of a student's parent if the parent requests from the school that the student's covered information held by the operator be deleted, so long as the deletion of the covered information is not in violation of State or federal records laws."

As such, we recommend the addition of the following subitem under III(a):

[Delete, within a reasonable time period, a student's covered information if either a school or the district requests deletion of such covered information under the control of the school or the district, unless a student or his or her parent consents to the maintenance of the covered information.](#)

We also recommend the addition of the following subitem under VI(c):

[Parents have the right to make a request to the school that his or her student's covered information held by an operator be deleted, so long as the deletion of the covered information is not in violation of state or federal records laws. Upon a parent making such a request, the school shall then make, on behalf of the parent, the request to the operator to delete such covered information.](#)

Furthermore, although it is not required under PA-101-516, we urge the district to consider implementing as part of this policy or an update to this policy, a requirement that operators agree to an annual deletion of non-longitudinal data (*cf.* this documentation from [Riverside \(IL\) District 36](#) and [Montgomery County \(MD\) Public Schools](#).)

Validation of software

The Information Security department should evaluate software not only for whether the operator maintains reasonable security procedures and practices, but also whether the software

complies with any privacy practices that PA-101-516 or other state or federal laws require or prohibit. This would include verification of what covered information is being collected; whether and how it is stored; if it will be used non-preK through 12 purposes; and whether parents will be able to exercise their rights to inspect, correct and request copies or deletions of covered information. We recommend the following modification of subitem IV(a)3b1:

Information Security will validate that the ~~vendor-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 and verify that the software complies with the requirements of the Student Online Personal Protection Act and any other federal and state privacy laws.

Parents' right to know

Subitem VI(c)2 says "Parents have the right to know which authorized software are being used in the classroom..." We recommend that this language is broadened to clarify that parents have the right to know how their children's data is being collected, stored and processed whether it is for the purpose of classroom instruction or another preK through 12 school purpose:

Parents have the right to know which authorized software are being used ~~in the classroom~~ to collect, store and process their child's covered information and to consent to the use of authorized software.

District auditing of authorized software

Subitem VI(a)1 places the locus of responsibility at the school level for auditing whether unauthorized or prohibited software are in use: "The principal must ensure teachers and staff are using authorized software." We recommend that the district create a district-level procedure to audit this and, to facilitate such an audit, require that the school maintain its own inventory of what software is in use by school personnel. This will have the added benefit of assisting in keeping parents informed of how their child's covered information is used. We recommend subitem VI(a)1 be modified as follows:

The principal must maintain an inventory of software in use by the school in order to ensure teachers and staff are only using authorized software.

Furthermore, we recommend that an additional item be inserted under Section V:

The district will, no less than annually, audit school software use to assess whether prohibited or unauthorized are in use in violation of this policy.

Notification of parents of breaches

Parents have the right to be notified about any breach of their child's information whether it is maintained by an operator or by the school. We recommend that the language of subitem VI(c)3 be modified to match more closely that of PA-101-516:

Parents have the right to be notified by the school or district of a breach by an operator of the student's covered information. The school or district shall notify, no later than 30 calendar days after receipt of notice of a breach by an operator or determination that a breach has occurred, the parent of any student whose covered information is involved in the breach; investigation and remediation expenses incurred will be allocated between the operator and the district.

Website posting of breaches

PA-101-516 requires that the schools or districts must maintain a list of breaches of student information whether held by the school or an operator on their website. Therefore, we recommend the addition of an item to the list under Section VII as follows:

A list of any breaches of covered information maintained by the school and any breaches of covered information maintained by an operator that includes, all of the following information:

1. The number of students whose covered information is involved in the breach, unless disclosing that number would violate the provisions of the Personal Information Protection Act.
2. The date, estimated date, or estimated date range of the breach.
3. For a breach of data maintained by an operator, the name of the operator.

Website posting of procedures to carry out student and parent rights

PA-101-516 also requires that the schools or districts post on their website a written description of the procedures that a parent may use to carry out the parent and student rights enumerated under Section 33 of the public act. As such, we recommend the addition of an item to the list under Section VII as follows:

A written description of the procedures that a parent may use to carry out the rights enumerated under SOPPA, including 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.

Prohibiting operators from requiring separate agreements that violate SOPPA or other privacy laws

Finally, we recommend that language be added to both Items III(b) and VI(c) that would clarify the requirement that operators may only receive covered information under the terms set in a written agreement with the district. The policy should state explicitly that under no circumstances shall students or parents be compelled to enter into an individual written agreement with an operator for a preK-12 student purpose and any optional agreement should not include terms that violate state or federal privacy laws. If a parent is asked for authorization or consent, it should be provided under an agreement between the school (district) and the parent, not the operator.

Currently, many district students are required to enter into individual agreements with operators in order to receive classroom instruction, complete and submit homework or participate in required assessments. These are often in the form of click-wrap agreements where a student must agree to terms and conditions in order to use an online site or application. Besides the fact that we feel it is deeply problematic for minors to be compelled to enter contracts with third parties in order to receive public education, it is also problematic because the status of these agreements and their terms are only weakly constrained under state or federal student privacy laws currently in effect (i.e. prior to the effective date of PA-101-516, July 1, 2021).

However, it is clear that the legislative intent of the Illinois General Assembly underlying Sec. 26(2) of PA-101-516 was to require that *any* transfer of students' covered information to operators for school purposes take place under a written agreement between the operator and the school (district):

"A school may not...[s]hare, transfer, disclose, or provide access to a student's covered information to an entity or individual, other than the student's parent, school personnel, appointed or elected school board members or local school council members, or the State Board, without a written agreement"

And, this requirement was stipulated because, under Section 15(4), such written agreements must meet a list of criteria that will themselves ensure that the prohibitions and requirements of PA-101-516 are being met, e.g. that students' data will be held securely at all times, not used for commercial purposes, allow for parents to exercise their rights of inspection, correction and deletion, etc.

If students' covered information is being shared with entities outside the auspices of the written agreement with the school or district, there is no way to know whether the provisions of PA-101-516 are met, much less enforce them if they are not.

As such, we recommend the following subitem be included under the list of operator prohibitions in III(b):

Requiring that a student or parent enter into a separate agreement with the operator in connection with any software provided by the operator via a written agreement with the district as regulated under IV(b), such that the separate agreement includes any terms that:

- (1) restrict the rights of the parent and/or student under state or federal privacy laws and/or
- (2) allow the operator to violate the terms of its written agreement with the district as to the collection, use, disposition or deletion of the student's covered information.

We also recommend the inclusion of this subitem under VI(c):

No parent nor student shall be compelled to enter into a written agreement or agree to terms of use with an operator in order for the student to participate in an activity with a preK through 12 school purpose, such that the agreement or terms of use restrict the parent and/or the student's rights under state or federal privacy laws or allow the operator to violate the terms of its written agreement with the district as to the collection, use, disposition or deletion of the student's covered information. Any such agreement entered into in violation of this subitem is void and unenforceable as against public policy.

Submitted,

Cassie Creswell, director
on behalf of Illinois Families for Public Schools