

Student Online Personal Protection Act

POLICY TEXT:

I. SCOPE OF THE POLICY: This policy outlines how Rockford Charter School Organization (hereinafter “Jackson Charter School”) will comply with its responsibilities under the Student Online Personal Protection Act (hereinafter “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. This policy summarizes the parent rights under SOPPA.

II. DEFINITIONS:

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

b. 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 K through 5 school purposes.

2. Created by or provided to an operator by an employee or agent of a school or school district for K through 5 school purposes.

3. Gathered by an operator through the operation of its site, service, or application for K through 5 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.

c. 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.

d. Educational Technology means educational software, electronic or online tools used by schools to improve student engagement, knowledge retention, individual learning or collaboration.

e. K through 5 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.

f. 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 K through 5 school purposes and was designed and marketed for K through 5 school purposes.

g. 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.

h. 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.

i. 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 school, 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. Delete, within a reasonable time period, a student's covered information if the school requests deletion of covered information under the control of the school, unless a student or his or her parent consents to the maintenance of the covered information.

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 K through 5 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 K through 5 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 advertising.

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. 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.

V. RESPONSIBILITIES FOR USING AUTHORIZED SOFTWARE:

a. School Use Procedures

1. The principal must ensure teachers and staff are using authorized software.

b. Teacher and Staff Responsibilities

1. Teachers and staff must receive approval from the principal prior to using authorized software.

3. Teachers and staff are prohibited from entering into agreements for any software or requiring students to do so.

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 when outlined in the guidelines consent to the use of authorized software

3. Parents have the right to be notified by the school of a breach of covered information.

VI. WEBSITE POSTING:

The school is responsible for posting relevant information on the school website.

a. Annually post a list of all operators of online services or applications utilized by the school.

b. Annually post all data elements that the school collects, maintains, or discloses to any entity. This information must also explain how the school uses the data, and to whom and why it discloses the data.

c. Post contracts for each operator within 10 days of signing.

d. Annually post subcontractors for each operator.

e. Post the process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.

f. Post data breaches within 10 days and notify parents within 30 days.

g. Create a policy for who can sign contracts with operators.

h. Designate a privacy officer to ensure compliance.

i. Maintain reasonable security procedures and practices. Agreements with vendors in which information is shared must include a provision that the vendor maintains reasonable security procedures and practices.

VII. 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.

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