Student Data Privacy

Board of Education meeting
9/21/2021

The vision of Roselle District 12 is to prepare students to ethically engage in our global society.

Student Data Privacy

Photo by Christopher Scholz on Flickr

The vision of Roselle District 12 is to prepare students to ethically engage in our global society.

Student Data Privacy

Photo by Christopher Scholz on Flickr

Student and child privacy laws work to ensure that:

- information about a student is used fairly
- information about a student is used only for its intended purpose and not for unwanted or unanticipated purposes
- students are not coerced into divulging personal information
- students are not exposed to deceptive messages

Student Data Privacy

Photo by Christopher Scholz on Flickr

Children's Privacy Protection and Parental Empowerment Act	prohibits the sale or purchase of personal information of a child under age 16 without parent/guardian consent, unless an exception applies
Local Records Act	provides requirements for how school districts maintain day-to-day recordkeeping
NSLA: The National School Lunch Act	governs school lunch programs, including provisions related to protecting financial data submitted as part of free and reduced lunch applications

Student Data Privacy

Photo by Christopher Scholz on Flickr

ISSRA - Illinois School Student Records Act	ensures parent/guardian access to their child's records and the confidentiality of student records and the information in those records
PPRA - The Protection of Pupil Rights Amendment	ensures that students are not coerced into divulging certain personal information and restricts the administration of surveys, analyses, or evaluations to students that concern specified protected topics, and requires notification to parents and parental consent when information is collected related to those topics.

Student Data Privacy

Photo by Christopher Scholz on Flickr

Right to Privacy in the School Setting Act	requires that schools: • may not request or require a student to provide a password or other account information to gain access to the student's account or profile on a social networking website. • MAY require the student to cooperate in an investigation if there is specific information about activity on the student's social media account that violates a school disciplinary rule or policy, including requiring the student to share the content of the social media site.

Student Data Privacy

Photo by Christopher Scholz on Flickr

IDEA: The Individuals with Disabilities Education Act	ensures that students with disabilities are given an appropriate education that is tailored for their needs. Since this requires collecting very sensitive personal information, the law specifies some additional privacy protections to ensure that this information is not used for other purposes
MHDDCA - Illinois Mental Health & Developmental Disabilities Confidentiality Act	governs the confidentiality of communications and records concerning mental health or developmental disability services provided to a student by school personnel who meet the definition of a “therapist”

Student Data Privacy

Photo by Christopher Scholz on Flickr

CIPA: The Children's Internet Protection Act	provides federal funding to schools that monitor and filter internet content and requires that schools teach students about digital citizenship and staying safe online. Though it is not directly a privacy law, it hits on many aspects of privacy since schools will have to determine the appropriate amount of monitoring and filtering as well as cover protecting personal privacy as part of the digital citizenship curriculum
FERPA - Family Educational Rights and Privacy Act	ensures that information about a student is used fairly by providing notice to parents about their rights toward student data

Student Data Privacy

Photo by Christopher Scholz on Flickr

COPPA - Children's Online Privacy Protection Act	regulates websites and online applications that collect information from children to ensure that they are not following deceptive practices. In general, these operators are required to provide notice and gather verifiable parental consent before collecting information from a child. Under the law, schools are allowed to provide consent in the place of a parent, provided that the website or online application only uses the information collected for educational purposes.

Student Data Privacy

Photo by Christopher Scholz on Flickr

New Additions

- provide further requirements and safeguards related to student data shared with websites, online services, and applications
- require more transparency about what data schools collect and what it is used for
- require that schools and vendors meet certain data security standards
- require notification to parents in the event of a data security breach

Student Data Privacy

Photo by Christopher Scholz on Flick

SOPPA - Student Online Personal Protection Act (effective 7/1/21)	requires that schools: • School districts must have a signed data privacy agreement with any edtech tool (operator) PRIOR to use with students • School district must publicly post a list of all edtech digital tools

Operators Must:	Operators Must Never:
• Implement reasonable security practices • Delete a student's information on request • Publicly list the types of information collected • Notify School in the event of a breach	• Engage in targeted advertising • Amass a profile for non-school purposes • Sell or rent student information • Disclose student information

Student Data Privacy

Photo by Christopher Scholz on Flickr

New Procedures

- App request form
- COPPA compliance
- Vetting process
- Data privacy agreement
- Required resources posted
- Approved for use

Copy of Illinois-National Data Privacy Agreement

Student Data Privacy

AIPhoto by Christopher Scholz on Flickr

PRIVACY EVALUATIONS

Copies of Privacy Policies

Written Agreements

Approved Vendor List

Staff access

Parent access

How can we provide all of this in one place?

Rationale for approval/denial

Vendor third party affiliates

A PLACE TO REQUEST SOFTWARE

Breach notifications

Student Data Privacy

Photo by Christopher Scholz on Flickr

Learn Platform

- Roselle District 12 website sd12.org
- For Parents tab
- Data Privacy in dropdown menu
- Data Privacy Agreements

Student Data Privacy

Photo by Christopher Scholz on Flickr

Besides data privacy what else is D12 doing to keep students safe online?

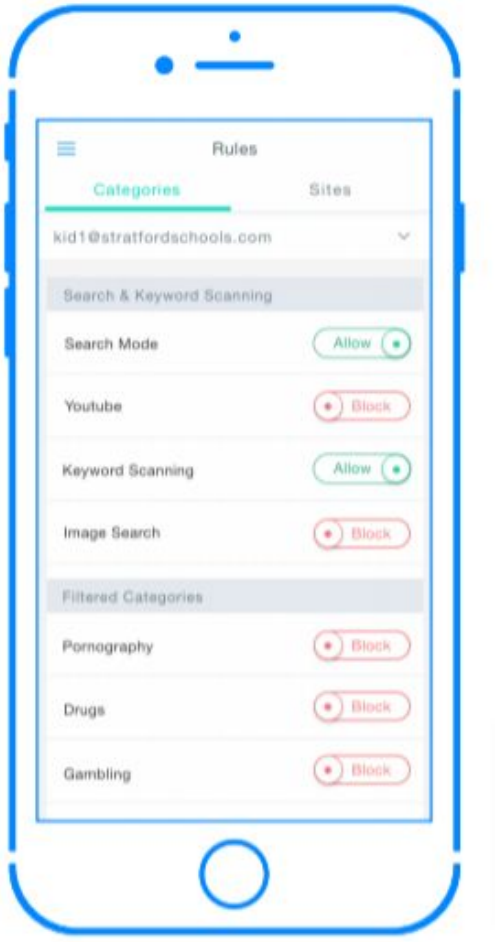
- Securly Monitoring
- Risk Assessment Protocols
- Securly Chrometools
- Securly Home

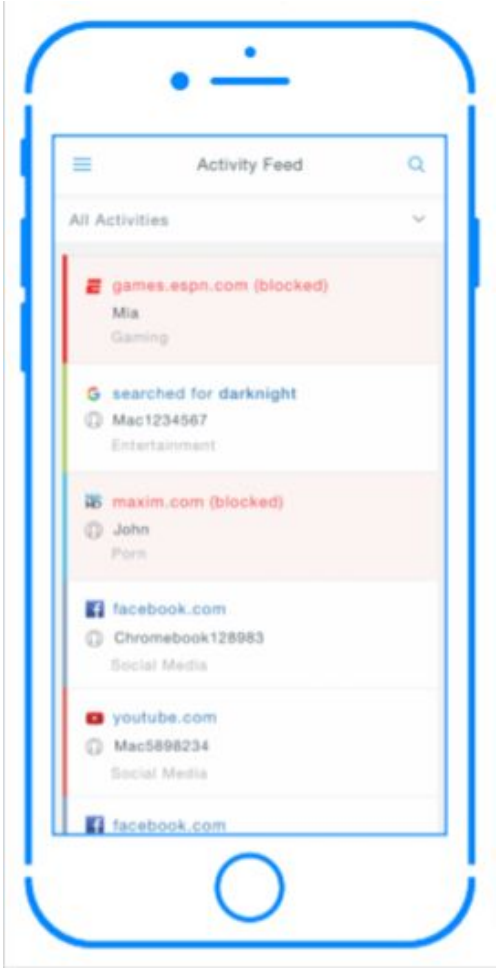
	Clarifying Risk	Analyst Action
Low Risk	Activity flagged	Analyst should not take action at this time. If additional information comes through, re-assess and take into account this previous report.
	No direct threat present	
Moderate Risk	Student exhibiting clear distress	Analyst should notify, via email, the emergency contacts as indicated by the district. Email should indicate that the threat does not appear to be serious, but we are notifying the district to make them aware.
	Threat present	
	Threat is vague and indirect but may be repeated or shared with multiple people	
	Information about threat or threat itself is implausible or lacks detail	
	Threat lacks realism or is repeated with variations. E.g. "I'm gonna set off a nuclear bomb every Monday!"	
	Content of threat suggests threatner is unlikely to carry it out	
Increased Risk	Threat present	Analyst should notify, via email, the emergency contacts designated by the school. Email should indicate the threat appears to be serious, but not imminent.
	Threat is vague, but direct, or specific but indirect (vague/specific in terms of plans, direct or indirect in terms of target)	
	Repeated or shared multiple ways (e.g. email, text, FB)	
	Threat likely to be repeated with consistency (may try to convince listener they are serious)	
	Information about threat or threat itself is consistent, plausible or includes specific detail of a plan (time, place, etc.) but NOT set within the next 24 hours; often with steps already taken. e.g. "I read about how to build bombs online. I've ordered some stuff that I need, but it won't be here for awhile. I should be ready when the school has that award assembly next month."	
	Content of threat suggests threatner may carry out, but not within the next 24 hours	
Extreme Risk	Threat made or present	Analyst should notify, via SMS or phone, the emergency contacts designated by the school. Based on the urgency of timing, if there is no response, every effort should be made to notify law enforcement.
	Threat is concrete (specific and direct)	
	Repeated or shared multiple ways (e.g. email, text, FB)	
	Information about threat or threat itself is consistent, plausible or includes specific detail of a plan (time, place, etc.) set within the next 24 hours; often with steps already taken. E.g. "Don't go to the assembly tomorrow. I've hidden enough bombs in the auditorium to teach everyone a lesson about messing with me."	
	Threat may be repeated with consistency	
	Content of threat suggests threatner will carry it out (reference to weapons, means, target) within the next 24 hours	

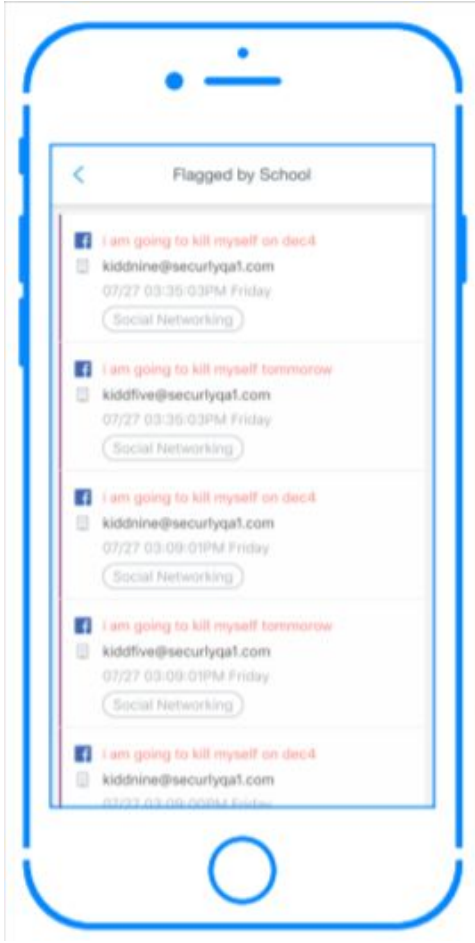
Student Data Privacy

Photo by Christopher Scholz on Flickr

Securly Home - Rules, Activities, Flags



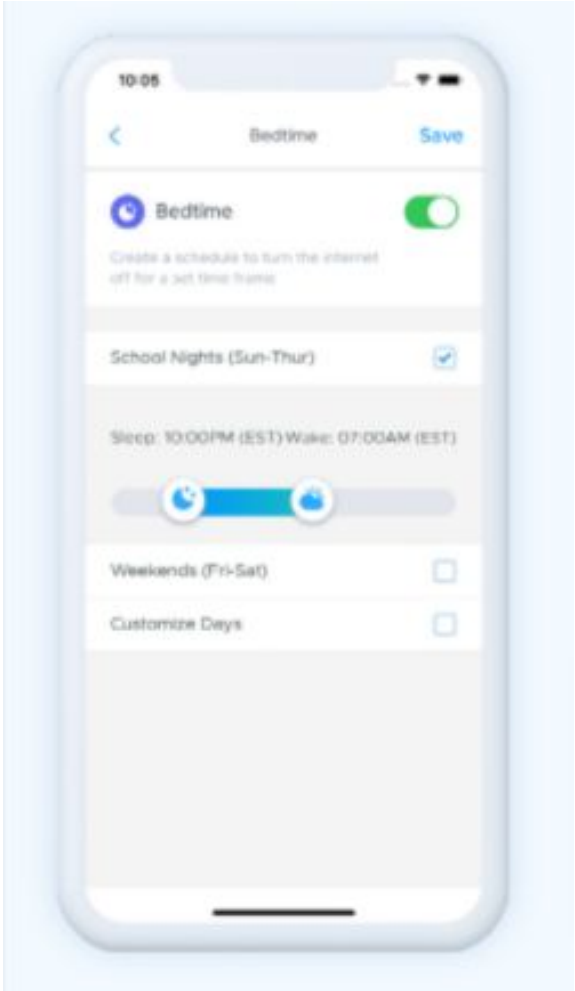


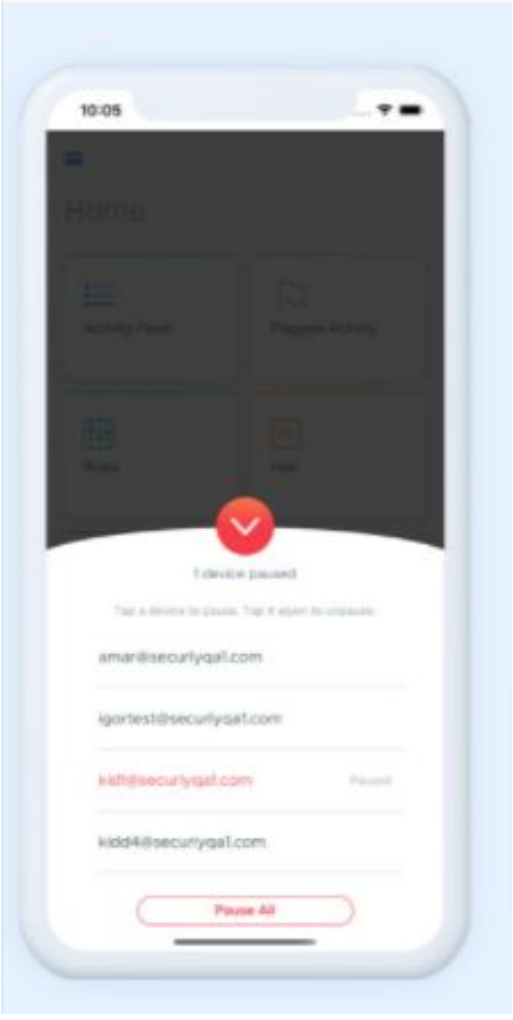


Student Data Privacy

Photo by Christopher Scholz on Flickr

Securly Home - Offline Schedules, Internet Pause





More information, resources, and Parent University information coming soon!

Student Data Privacy

Photo by Christopher Scholz on Flickr

Thank you for joining us on the mission to keep our students safe!