The K-12 Privacy Policy Guide: How to Quickly Spot Red Flags

Produced in partnership by:

PIPC | Lightspeed Systems®

Introduction

Using technology in classrooms can transform the learning experience and provide immense benefits for both students and educators. But before it's used, it is imperative to ensure that our students' information and privacy are protected.

One of the main steps to doing that is reviewing an app's privacy policy before requesting approval to use it with your students. We understand that deciphering a privacy policy can be a hard task–privacy policies are often long, hard to read, and full of legalese. Furthermore, schools are often overwhelmed with requests to vet different technologies, many of which do not sufficiently protect student data. This resource is meant to help educators quickly find big problems in privacy policies that would likely restrict the tool from being used with students.

In this guide we list common "red flags" to look out for in privacy policies. This is not a comprehensive list of potential problems, but an overview of large issues that can be found in a quick, five-minute scan of a policy. If any of these are in a privacy policy that you are reviewing, it is unlikely that it is appropriate to use that technology with your students. If that's the case, you can always check or request if your school has or can enter into a separate privacy-protective contract with the technology company.

To help find potential "red flags" in privacy policies, we have listed "key search terms" that you can use to filter through the document you are reviewing. These search terms should help you quickly navigate through privacy policies by taking you directly to potential red flags.

This is only the first step in the technology vetting process. After checking that the privacy policy does not contain the following red flags, teachers must follow their school's official process for vetting technologies before using them with students. These policies and procedures tend to vary by school, so check to see if your school maintains a list of the technologies that have already been formally approved for use with students and to find out how to request an official review of other technologies.

Before you begin

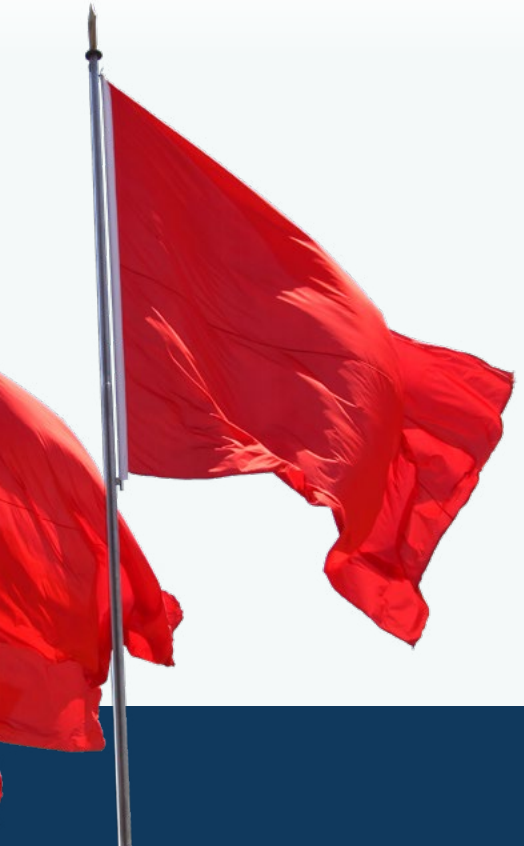
Does the service offer a product specifically for education? Many technology companies offer two versions of the same platform, one that is broadly directed to children and parents and one that is offered specifically for schools. If the technology you are considering offers an education specific platform, make sure you are reviewing their education-specific privacy policy.

Overview of Components

Data Sharing

There are many legitimate, functional reasons for a technology provider to share student data with third parties. For example, nearly all platforms share data with the third party hosting the website, or rely on a cloud service provider for storage. However, it's important to ensure that this sharing happens in a privacy-protective way. Using technologies that do not have clear, privacy-protective policies for sharing student data with third parties may introduce unnecessary risk and compromise trust between schools and the communities they serve.

Red Flags:



- **Third Parties:** The policy does not specify or limit what third parties they may share student data with.
- **Non-Educational Purpose:** The policy permits sharing student data for purposes unrelated to education, such as for advertising or marketing.

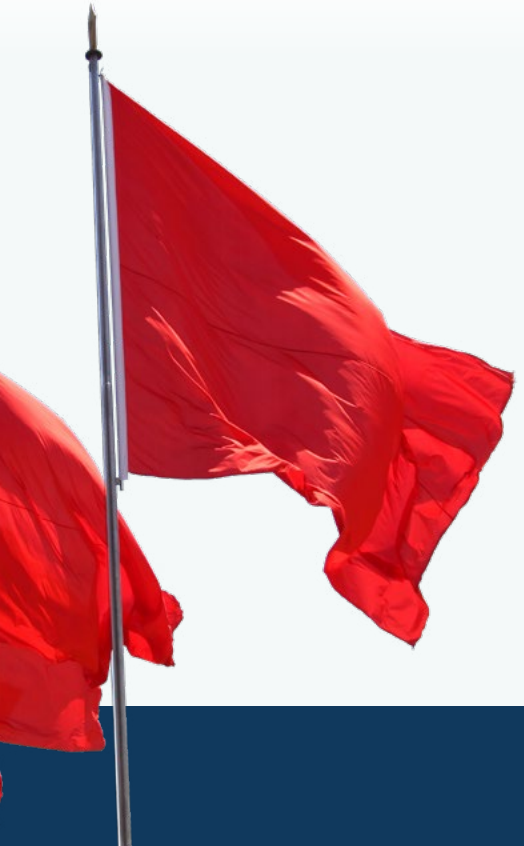
Key Search Terms

- Third parties
- Partner
- Share

Data Usage

Companies may want to use student data for non-educational purposes that are not necessary to provide the service and may put student data at risk. Limiting data usage helps ensure that student data is used responsibly, only for the purposes the school intends, and with students' best interests in mind. For instance, the protective privacy policy may say "we create user profiles only for authorized educational purposes."

Red Flags:



- **Targeted, Behavioral, or Personalized Advertising:** The policy permits the platform to use student data for targeted advertising.
- **Commercial Purposes:** The policy states that student data may be used for commercial purposes, such as developing new products.

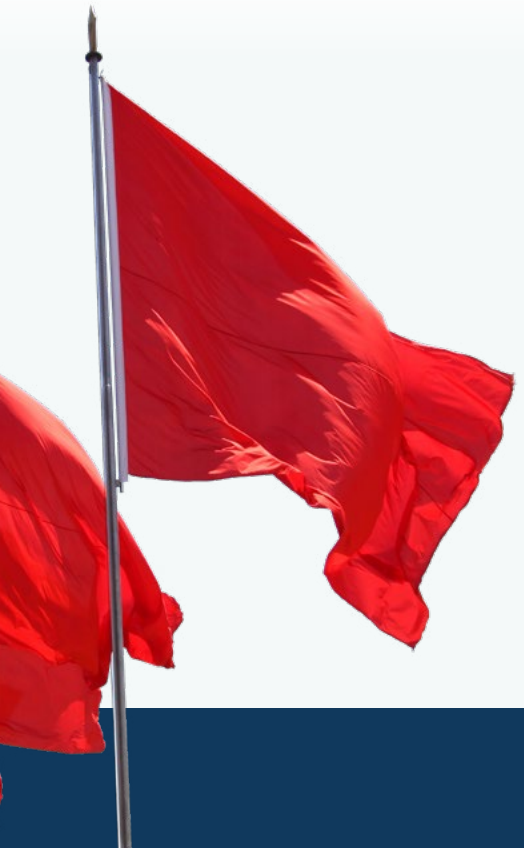
Key Search Terms

- Advertise
- Develop

Data Ownership

Data owners often have the final say over how data is safeguarded, used, and ultimately destroyed. Schools, rather than technology companies, need to be in control of student information so that they can ensure strong data governance practices are in place to protect student data.

Red Flags:



- **Exclusive Ownership:** The policy states that the platform owns all data generated or collected within the platform, including student-generated content and student personal information.
- **Unlimited License:** The policy grants the platform an unrestricted license to use, modify, or distribute student data for any purpose.
- **Lack of Controls:** The policy does not mention how control can be exercised over data collected from students, such as the ability to access, correct inaccuracies, or delete information.

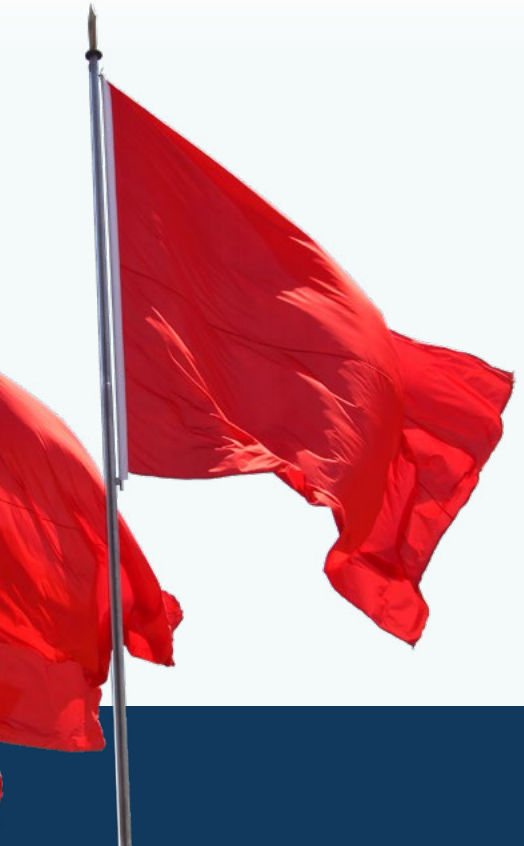
Key Search Terms

- Control
- License

Data Retention

Keeping student data for longer than necessary increases the risk that student data may be improperly accessed, used, or shared.

Red Flags:



- **Lack of a Data Retention Limit:** The policy does not set a time limit for how long student data can be retained or permits the platform to retain student data indefinitely.
- **Lack of Data Deletion Procedures:** The policy does not include any provisions or procedures for deleting student data upon request or at the end of the platform's usage.

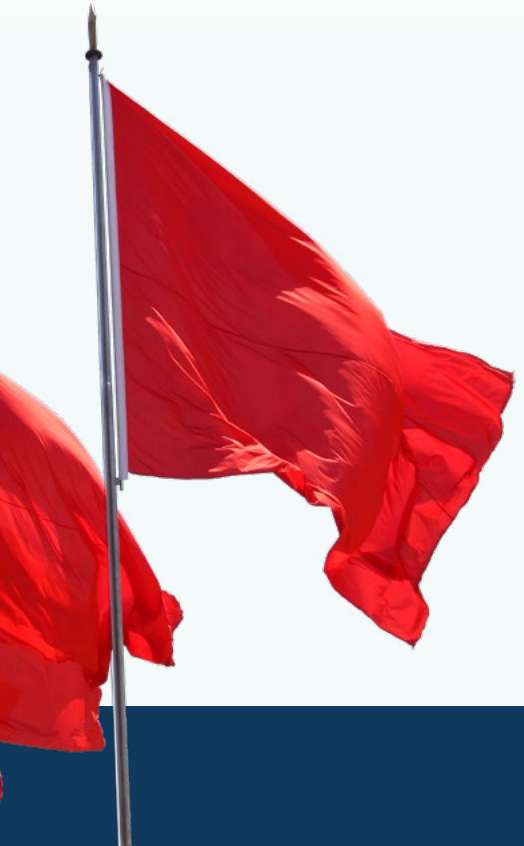
Key Search Terms

- Retain
- Delete/deletion

Security

Technology platforms need to have measures in place to protect student information from unauthorized access and use. Ensuring that technology platforms have appropriate security measures in place is very important to safeguarding student data against potential cyber threats.

Red Flags:



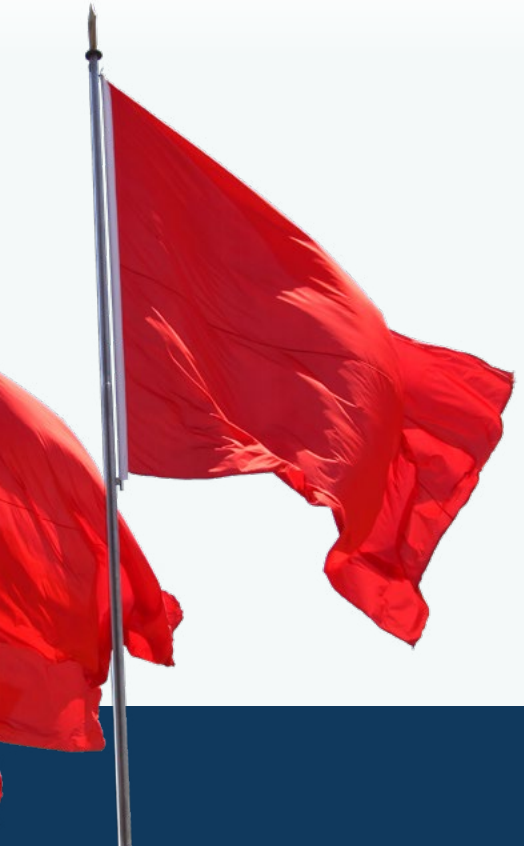
- **Lack of a Data Security Policy:** The policy does not mention specific security measures in place to protect student data.
- **Waiver of Liability:** The policy waives all liability for security breaches.

Key Search Terms

- Protect/Protection
- Breach
- Encryption

Updates and Changes

Changes to a technology's privacy policy may remove important privacy and security protections for student data. Schools must be notified of any changes made to a technology's privacy policy so they can assess whether their continued use of the platform with students still aligns with required student privacy standards.



Red Flags:

- **Lack of Notice:** The policy allows the platform to make material changes to their privacy policies and data handling practices without providing notification.

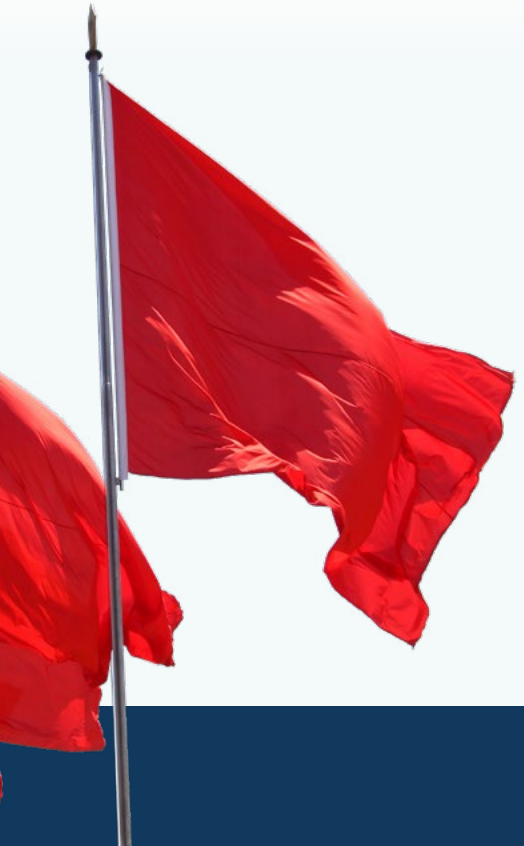
Key Search Terms

- Update
- Notice/Notification

Data Collection

Some companies actively seek and collect more data from users than is necessary to provide their product, putting students at risk of sharing more information with companies than the school intended. Technology platforms should only be allowed to collect student information that they actually need to provide their product.

Red Flags:



- **Lack of Data Minimization:** The policy does not state that they only collect the minimum amount of data necessary to provide the service.
- **Unrelated Data Categories:** The policy permits the platform to collect student data that seem unrelated to the service without explaining why, such as a geometry app collecting information about participation in extracurricular activities without stating the reason they need this data to run the app.

Key Search Terms

- Collect
- Minimal/minimum

Conclusion

As technology continues to advance and create new opportunities to enhance student learning, it is essential for educators and schools to prioritize privacy protection when utilizing edtech products in the classroom. This resource aims to assist schools in the vetting process by equipping educators with the baseline knowledge they need to quickly review an edtech product's privacy policy before submitting it for official review. Our hope is that all K-12 decision-makers can use this resource as a guide to spotting the major privacy pitfalls they should be on the lookout for when considering using edtech products with students. This resource is not meant to make everyone an expert in data privacy but rather is intended to illustrate ways student privacy can be put at risk that would likely restrict the tool from being used with students.

Protecting student privacy in the education context can be a difficult task, but it is necessary to ensure the safety and well-being of students. By taking 5 minutes to look over an edtech product's privacy policy before submitting it for review, educators can play a crucial role in the district's technology vetting process and protect student privacy while providing a technology-enhanced education.

The Public Interest Privacy Center (PIPC) is a nonprofit organization that equips stakeholders with the insights, training, and tools needed to cultivate effective, ethical, and equitable privacy safeguards for all children and students. Our vision is that high-impact stakeholders at every tier will have the information and tools necessary to protect all children's fundamental right to privacy. By educating and equipping high-impact groups and fostering a culture of privacy, PIPC will help create an environment where all children will enjoy privacy-protected benefits of emerging technologies and data use.

www.publicinterestprivacy.org

Lightspeed Systems® is dedicated to providing time-saving solutions and empowering districts to focus where it matters most—students and learning. Lightspeed provides one integrated platform of cloud-managed solutions: Security & Compliance, Safety & Wellness, and Engagement & Impact, purpose-built for school networks and devices. Headquartered in Austin, Texas, Lightspeed serves more than 23 million students using 15 million devices in 31,000 schools throughout 42 countries.

www.lightspeedsystems.com

The K-12 Privacy Policy Guide: How to Quickly Spot Red Flags

Produced in partnership by:

www.publicinterestprivacy.org

www.lightspeedsystems.com