Legal Compliance

As the owner and developer of ClassCabinet, I take the security of user data very seriously. I am constantly working both to improve data security and to ensure that ClassCabinet is compliant with legislative requirements regarding the security and student data. The purpose of this document is to provide a summary of the laws governing the use of student data online, and how ClassCabinet follows those laws.

Last Updated: 29 March 2023

What are the Governing Laws?

At the Federal level, there are two key pieces of legislation that set standards for student data. First is the **Family Education Rights and Privacy Act**, known as **FERPA**. The second is **Protection of Pupil Rights Amendment**, known as **PPRA**. I have provided links to both of these documents here, along with a link to the Federal Department of Education web site on student data security.

- Federal Department of Education home page regarding security of student data
- FERPA
- PPRA

Because ClassCabinet is run in Colorado, there are two additional key pieces of state legislation that must be considered in conjunction with FERPA and PPRA. The first is **The Student Data Transparency and Security Act**, and the second is the **Data Breach Notification Law**.

Information about these laws can be found on the Colorado Department of Education (CDE) web site using the two links provided here.

- CDE Data Privacy and Security Home Page
- CDE Links to Resources for Data Privacy

What are ClassCabinet's Policies?

With respect to ClassCabinet, I have developed three key policy documents regarding data and security. I have worked very hard to make sure that ClassCabinet not only follows the laws, but exceeds the expectations set forth therein.

1. The **Privacy Policy** describes they type of data collected, how it used, who can see what data, and how ClassCabinet uses the data. As a summary, all user data on ClassCabinet is only used for education purposes, will never be used for any other purpose, and will not be disclosed to anyone who does not have a legal right and education need to the data. The policies set forth in the Privacy Policy have been carefully compared with the following to ensure that they meet every legal standard:
    a. the Model Terms of Service provided by the Department of Education,
    b. The School Service Contract Providers Obligations Under the Student Data Transparency and Security Act
    c. The Data Breech Notification Law
2. The **Terms of Service** describes expectations of ClassCabinet users with respect to security and privacy of the data stored there. By agreeing to the terms of service, users agree to let ClassCabinet store their data so long as it is only used in the manner described in the Privacy Policy. They also agree to honor the security of the information stored there, and to only use ClassCabinet for legitimate educational purposes.
3. The **Security** document provides a summary of the measures used to ensure that your information is secure. It is an extract of the Security section from the Privacy Policy. The same information is also found below.

Summary of How ClassCabinet is Compliant with State and Federal Policy

FERPA is the center-piece legislation regulating the disclosure of student data, which it refers to specifically as Personally Identifiable Information, or PII. Because teachers working for a school district have a clear educational need to access and generate data pertaining to their students, they have a legal right to access student data [See FERPA 99.31.(a)(I)(i)A)]. However, except under the exceptions described below, no individual with access to student data is to disclose that data to other individuals, and must take measures to ensure that they do not do so. With respect to data stored online, FERPA simply states:

"An educational agency or institution must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses personally identifiable information from education records." FERPA 99.31(c).

The "reasonable methods" requirement is admittedly a bit vague. Thankfully, the Department of Education has provided guidance on best practices for securing data online, and authentication of users. ClassCabinet has implemented the following security and authentication procedures, which in many cases are more stringent than the best practices suggested by the Department of Education.

- Access to every ClassCabinet page is redirected to take place over a secure connection using HTTPS over TLS protocol.
- Every user's initial sign in on unrecognized devices requires a private username, encrypted password, and 2-factor authentication using the email registered with the relevant educational institution.
- Persistent sign-ins on trusted devices authenticate through local cookies.
    - Individual sessions persist for 1 day, after which time the user must re-enter their password.
    - 2-factor authentication persist for 7 days, after which time the user must re-authenticate.
- Every page other than the public facing pages, which do not require sign-in and do not display user data, authenticates the user credentials and user type for the information being accessed; authentication failure returns an error and ends data transfer.
- Best practices are employed in coding techniques to prevent attacks such as SQL injection.
- ClassCabinet has contracted with Sucuri, an independent security platform, which enhances ClassCabinet security by providing services such as firewall protection, malware detection and removal, regular security scans, reports on any security threats and suspicious activity, and more.

With respect to the disclosure of student PII to third parties, FERPA [99.31 (a)(1)(B)(1-3)] makes exceptions for disclosures of data to third parties under three conditions

1) they perform educational services typically performed by employees, making the third party a functional employee of the district.

2) The data is under the direct control of the educational agency with respect to the use and maintenance of educational records.

3) Is subject to the requirements found in subsection 99.33(a) of FERPA pertaining to the redisclosure of PII.

ClassCabinet meets requirement one because it provides teachers, students, and parents with tools whose only uses are educational. Per the ClassCabinet Privacy Policy and Terms of Service, any other use is forbidden and will not be tolerated. In this regard the PPRA is also relevant; the primary focus of this law is the use of student PII for research, advertising, and marketing. For these uses the individual or organization using the data for these purposes must receive parental consent before doing so. However, it notes that parental consent is not needed when student PII is collected with the exclusive purpose of developing, evaluating, and providing educational products or services for students or schools [20 U.S.C. § 1232h(c)(4)(A)]. Which precisely describes ClassCabinet's sole purpose.

With respect to the 2nd requirement, the Department of Education has provided guidance regarding requirements and best practices. Herein it is explained that the 2nd requirement is usually satisfied through legal assurances that the third party will follow all policies governing the "*access, use, and protection of the data*". It further states that the Terms of Service (and by extension the Privacy Policy) of the third party can be "*sufficient to legally bind the provider to terms that are consistent with these direct control requirements.*" Given that the ClassCabinet privacy policy meet all such provisions, it alone could satisfy this requirement. In Colorado, the Student Data Transparency and Security Act of Colorado recommends that these agreements be formalized with a written agreement between the school and the third party, which may also be true in other states. As the owner and developer of ClassCabinet, I am happy to do so whenever needed.

Regarding the third requirement, FERPA 99.33(a) states the following:

"(1) An educational agency or institution may disclose personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.

(2) The officers, employees, and agents of a party that receives information under paragraph (a)(1) of this section may use the information, but only for the purposes for which the disclosure was made." FERPA 99.33(a)

Because ClassCabinet data is stored on InMotion Hosting servers, they must held to this standard. In satisfaction of this clause, the InMotion hosting privacy policy states the following:

"How Company [InMotion Hosting] Uses and Shares Personal Information: Company strongly believes in both minimizing the data collected and limiting its use and purpose to only that (a) for which Company has been given permission, (b) as necessary to deliver the Websites or Products, or (c) as Company might be required or permitted for legal compliance or other lawful purposes." Privacy Policy 7.1

Furthermore, as required by California law (where InMotion Hosting is based), they have provided the opportunity to specifically opt-out of the resell or sharing of their user's information, and I have specifically done so.

FERPA further requires that parents and students have the ability to access their child's educational data. ClassCabinet satisfies this by creating accounts for all parents using the email that is registered with the school. Using the same authentication procedures described above, parents can access all information stored by ClassCabinet as it pertains to their child. I have in fact received many complements and thanks from parents for the clarity of the information that ClassCabinet provides.

FERPA and PPRA both assert strict requirements regarding the disclosure of student data for any purpose that is not solely educational, especially when it pertains to marketing and advertising. The ClassCabinet privacy policy clearly states that no information is shared with any third party for any purpose, most especially marketing and advertising.

The Data Breach Notification Law of Colorado also specifies that "*each entity in the state that maintains paper or electronic documents during the course of business that contain personal identifying information shall develop a written policy for the destruction or proper disposal of those paper and electronic documents containing personal identifying information."* I have accordingly also addressed this in the ClassCabinet privacy policy.

If you have any questions regarding your data or the information provided in this document, please contact me at help@classcabinet.com.

Sincerely,

Jason R Mayberry

Owner and Developer of ClassCabinet