Instructure Security and Operations

Canvas FERPA Compliance

Instructure, Inc.

June 22, 2013
1 FERPA COMPLIANCE

Canvas was built to comply with the Family Educational Rights and Privacy Act (FERPA) by design. Canvas is a hosted LMS solution that readily integrates with other campus systems to prevent unauthorized access to FERPA-protected data. Whether implemented as a standalone system or as a fully integrated component of the campus IT/IS infrastructure, Canvas provides educational institutions and agencies with multiple mechanisms and technologies to manage, enforce, and comply with the provisions of FERPA and to fulfill their responsibilities under its requirements.

1.1 FERPA Overview

FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools and institutions that receive funds under the applicable program of the U.S. Department of Education. FERPA provides students, and in some instances parents, the right to inspect their education records and some ability to control the disclosure of information contained in their education records.1

FERPA requires educational agencies, which disclose personally identifiable information from a student’s education record to other school officials, to use “reasonable methods” to insure school officials obtain access to only the education records they have legitimate educational interests in.2

Table 1–1 identifies key sections and requirements of the Family Educational Rights and Privacy Act (FERPA) and briefly describes how Instructure and the Canvas learning management system (LMS) comply.

<table>
<thead>
<tr>
<th>Item</th>
<th>FERPA Section</th>
<th>Requirements</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructure as a “School Official”</td>
<td>34 CFR § 99.31 (1)(i)(B)</td>
<td>(1) Performs an institutional service or function for which the agency or institution would otherwise use employees; and (2) Under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.</td>
<td>Instructure is under the direct contractual control by the agency or institution with respect to the use and maintenance of education records.</td>
</tr>
</tbody>
</table>

2 34 CFR § 99.31
<table>
<thead>
<tr>
<th>Item</th>
<th>FERPA Section</th>
<th>Requirements</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency or Institution Disclosure to Instructure as a “School Official”</td>
<td>34 CFR § 99.31 (a)(ii)</td>
<td>Education institution must use “reasonable methods” to make sure school officials have access to only education records they have legitimate educational interests in.</td>
<td>Provide Instructure only the information needed to serve its function. Access to educational records is dictated by course enrollment and role data provided by the institution. Access inside of a course can be further limited by groupings of students.</td>
</tr>
<tr>
<td>Requirement of Further Non-Disclosure</td>
<td>34 CFR § 99.33 (a)(1)</td>
<td>School can disclose information 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.</td>
<td>Contract with Instructure specifies that Instructure not disclose the information to any other party and otherwise in compliance with FERPA.</td>
</tr>
<tr>
<td>Permission settings within the Software</td>
<td>34 CFR § 99.30 (a)</td>
<td>Parent or eligible student shall provide a signed &amp; dated written consent before an educational agency or institution discloses personally identifiable information from the student’s educational records, except as provided in § 99.31.</td>
<td>Agency or institution can change the permissions settings within the software to allow for, or deny, access to certain types of users. (See below page 6)</td>
</tr>
<tr>
<td>Course Settings</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Agency or institution can change the course settings within the software to allow certain users to access the course. (See below page 7-8)</td>
</tr>
<tr>
<td>Account Settings</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Agency or institution can change the account settings within the software to allow only certain users to access features. (See below page 9)</td>
</tr>
<tr>
<td>Names, not potentially sensitive contact information are displayed in Canvas (security feature)</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Canvas displays students’ names in the course; however students’ email addresses or phone numbers will not be displayed. Students enrolled in the same course can contact one another, but the communication will be mediated through Canvas and students’ email addresses will not be disclosed.</td>
</tr>
<tr>
<td>Log off inactive users (security feature)</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Canvas automatically logs out users after a period of inactivity.</td>
</tr>
</tbody>
</table>
## FERPA Compliance

<table>
<thead>
<tr>
<th>Item</th>
<th>FERPA Section</th>
<th>Requirements</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser Session Logout</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Once a browser session is closed and a new browser is opened, Canvas will require the user to login again.</td>
</tr>
<tr>
<td>Authentication Integration</td>
<td>Same as above</td>
<td>Same as above</td>
<td>Single-sign-on is highly encouraged. All access to the system is dictated by the Institution-controlled identity system (SAML 2.0, CAS, LDAP, Shibboleth etc.).</td>
</tr>
</tbody>
</table>

### 1.2 Customization

Under FERPA, each school must define in their annual notification who constitutes a school official and what constitutes a legitimate educational interest. Because of this variation, Canvas provides settings that can be configured to conform to each school’s definitions. This document describes the various Canvas settings related to FERPA, the default settings, and the changes that may be made to these settings.

### 1.3 Permissions

One of the main FERPA-related tools available to educational agencies is the ability to define the permission settings for specific user roles in Canvas. Roles are established and communicated within Canvas by the type of course or section enrollment. The management of enrollments and the associated role permissions enable schools to specify what data each user can view. Both instructor and teacher’s assistant enrollments can be limited to student data in a section, which is a sub-group of the overall course enrollments. Enrollment data is typically furnished via integration with the institution’s student information system (SIS). The default permission settings can be changed to either allow or deny access to specific features and data.

To access the permission setting page in Canvas as shown in Figure 1–1, select “Permissions” from the dashboard’s left hand menu in a Canvas course. In addition to the user roles of Students, Teachers, and Course Designers, Canvas also has the predefined roles of:

- TAs – individuals who serve as a teacher’s assistants.
- Observers – individuals who have access to the course, but do not participate in the course.

---

3 34 CFR § 99.7
1.4 **Course Settings**

All data and course content is securely stored under an associated access control policy. Every time the data or content is accessed, this access control policy is consulted before access is granted to the requested resource. By default, Canvas only allows users enrolled in a course to view course content. With the growing need for OpenCourseWare and Open Content of educational resources, Canvas through the mechanism of these access control policies can safely permit the sharing of course content publicly while protecting and maintaining the privacy all personal and FERPA associated content. These policies support the sharing of continuously updated course content without compromising data security.

The procedures below step through the process for making a course public while keeping all the student data private and secure.

1. Click on “Courses” from the top-level navigation menu in the Canvas dashboard to display the course selection page. Select the course for which you would like to change the settings.
2. Select “Settings” from the left hand course menu to display the course details page as shown in Figure 1–2.
3. Click on the “Edit Course Details” button at the bottom of the course details page.
4. Select the box next to “Make this course publicly visible,” then click “Update Course Details” as shown in Figure 1–3.
1.5 Account Settings

1.5.1 Authentication Integration

Single-Sign-On (SSO) is configured at the account level. SSO gives the institution full control over which users are authenticated and how that authentication is performed. Role information is communicated with enrollment data via integration with the institution’s SIS. Supported identity protocols include LDAP, CAS, SAML 2.0, and Shibboleth, a profile of SAML.

1.5.2 Assessment Results in External Notifications

An educational agency can decide whether or not it will allow students to have the ability to opt-in to receiving grades by external notifications through email, SMS, or other communication channels. By default, when an instructor assesses submitted assignments, students can receive notifications that they have received a grade on a specific assignment, but the notification will not include the grade received. If the educational agency has selected this option, it will allow the student to consent or opt-in to receive the grade in the notification as well.

To change the default setting:

1. Click on the “Settings” tab located on the left hand menu of the dashboard.
2. By default, the Settings tab will be displayed as shown in Figure 1–4.
3. Click on “Students can opt-in to receiving scores in email notifications” and then click “Update Settings.”

![Account Settings](image-url)

Figure 1–4. Allowing students to opt into receiving grades in notifications.
Figure 1–5. Students can opt into receiving grades notifications in their account settings.

1.6 Other Default FERPA-related Features

Additional features in Canvas related to FERPA compliance include:

- Logging Off Inactive Users
  - Canvas will automatically logout the user after a period of inactivity.

- Browser Session Logout
  - Once a browser session is closed and a new browser is opened, Canvas will require the user to login again.

- Names, not potentially sensitive contact information, are displayed in Canvas
  - Canvas displays students’ names in the course; however students’ emails or phone numbers will not be displayed to other students. Users enrolled in the same course can contact one another, but the communication will be mediated through Canvas and users’ actual contact information will not be disclosed. The audit and record of communication is accessible by administrative accounts with appropriate permissions.