CourseNetworking as a 'School Official'

FERPA LAW SAYS:

34 CFR§ 99.31 Under what conditions is prior consent not required to disclose information?

(1)(i)(B) A contractor, consultant, volunteer, or other party whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided the outside party –

> 1. Performs an institutional service or function for which the agency or institution would otherwise use employees;

> 2. Is 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 re-disclosure of personally identifiable information from educational records.

CourseNetworking is under the direct contractual control by the agency or institution with respect to the use and maintenance of education records.

Agency or Institution Disclosure to CourseNetworking as a 'School Official'

FERPA LAW SAYS:

34 CFR§ 99.31 Under what conditions is prior consent not required to disclose information?

(a) An educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by § 99.30 if the disclosure meets one or more of the following conditions:

> **(ii)** An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section.

Provide CourseNetworking only the information needed to serve its function. Access to educational records is dictated by course enrollment and course role data provided by the institution and includes, name, course enrollment and role information and email address. Access inside of a course can be further limited by groupings of students.

Requirement of Further Non-Disclosure

FERPA LAW SAYS:

34 CFR § 99.33 What limitations apply to the re-disclosure of information?

(a)(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.

Contractual agreements with CourseNetworking specifies that CourseNetworking cannot disclose the information to any other party otherwise in compliance with FERPA. Third party tools may be integrated into CourseNetworking per the institution's request, and then the institution holds responsibility in regards to the disclosure of student information, account creation, etc.

Permission Settings within Software

FERPA LAW SAYS:

34 CFR § 99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31

Agency or institution can change the permissions settings within the software to allow for or deny, access to certain types of users. **(See Page 4-5)**

Account Settings

FERPA LAW SAYS:

34 **FR § 99.30** Under what conditions is prior consent required to disclose information?
(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31

Agency or institution can change the course settings within the software to allow certain users to access the course. **(See page 6)**

Names, not potentially sensitive contact information are displayed on CN (security feature)

FERPA LAW SAYS:

34 **FR § 99.30** Under what conditions is prior consent required to disclose information?
(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31

CourseNetworking displays students' names in the course and their CN Number; however, by default students' email addresses or phone numbers will not be displayed. They can choose to show this information. Students may network and contact one another or any other user on CN, but the communication will be mediated through CourseNetworking and students' email addresses will not be disclosed. Institutions can disable this feature.

Log off inactive users (security feature)

FERPA LAW SAYS:

34 FR § 99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31

CourseNetworking allows institutions to choose the time in minutes, days, or weeks in which the system automatically logs out users after a period of inactivity. By default, the system logs out users after 30 days of inactivity. **(See Figure 18 in "Other" Section)**

Authentication Integration

FERPA LAW SAYS:

34 FR § 99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31

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.) **(See page 15)**

Customization

Under FERPA, it is up to each individual school to define who constitutes a school official and what constitutes a legitimate educational interest. Because of this variation, CourseNetworking provides settings that can be configured to conform to each school's definitions. This document describes various CourseNetworking settings related to FERPA, the default settings, and the changes that may be made to these settings.

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 CourseNetworking. Roles are established and communicated within CourseNetworking by the type of course or section of enrollment. The management of these enrollments and corresponding role permissions allow schools to specify what data each user can view. Both by instructor and teacher's assistant enrollments can be limited to student data in a section, which is a subgroup of the overall 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 role settings from a course page in CourseNetworking as shown in **Figure 1**, select "Roster" from the left navigation menu in a CourseNetworking course. Then click on a gear icon next to any member's name and select "Change member role/permissions to view or change their predefined role. In addition, to the user roles of Students and Instructors, CourseNetworking also has the predefined roles of:

- TA's, Instructional Designers, Field Experts – All of the same permissions as an instructor except, cannot change member roles/permissions, cannot drop course members, have instructor selected limited access to GradeBook and DropBox.
- Observers – Treated like a student role, except they do not appear the in course GradeBook
- Content Editors – Instructor may assign content editors to manage the content on specific tasks.

Note: Names of Roles may be changed to meet an institution's needs – see **Figure 2**

Figure 1. Role Settings

Figure 2. User Role

Course Settings

Instructors can go to Course Basic Settings, see Figure 3, to set course access setting. They can make their course available to Public (everyone who obtains a CN number can join course) or restrict course access to members, see Figure 4, who have the course 4-digit PIN code or those invited by a course invitation email. Instructors can also choose "Only Me" and change to another access setting when they are ready to open up their course. Licensed Institutions can determine course enrollment by uploading a CSV file or through integration with their SIS. They can also disable instructors from changing course access 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.

The procedures below step through the process of making a course public while keeping all the student data private and secure.
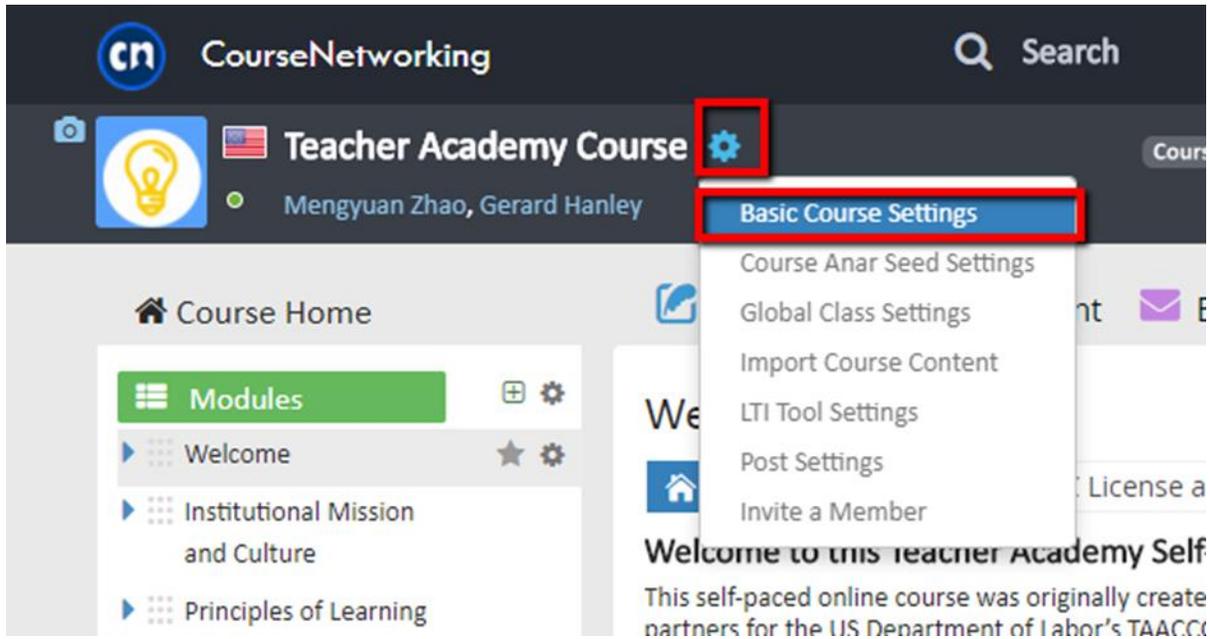
Figure 3. Course Settings
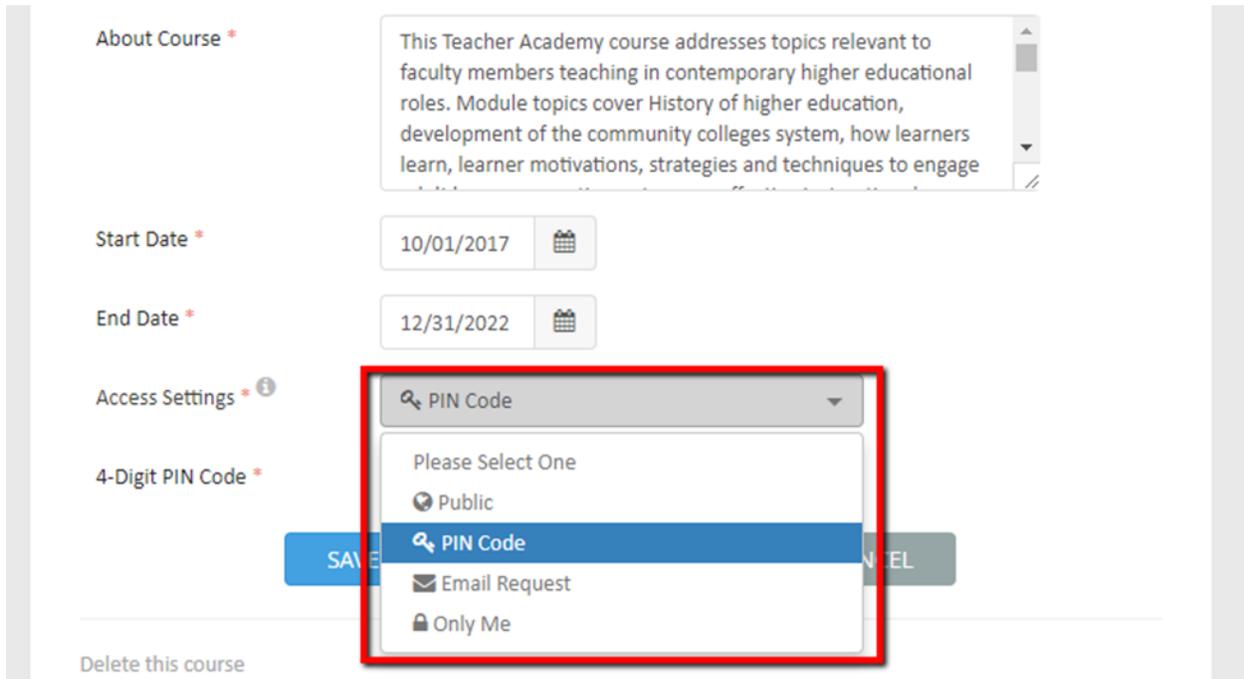
Figure 4. Course Settings

Global Class Settings

Can opt-in on a category basis, department basis, or keep secret.

Post Privacy Settings

1. Visibility Settings

On CN, users must select a visibility setting for each of their posts. By doing this, they tell the system whom they want to allow to view their content. CourseNetworking provides different options on different based on the different site pages. **Figure 5** shows post visibility options on the course page. Aside from selecting a post visibility setting, users can also check the box "Show in my CN ePortfolio" to display their post on their public ePortfolio. By default the box is unchecked.

Licensed institutions can disable certain post visibility options, such as "Visible to All CN Members" and "Visible to This Course and Global Class."
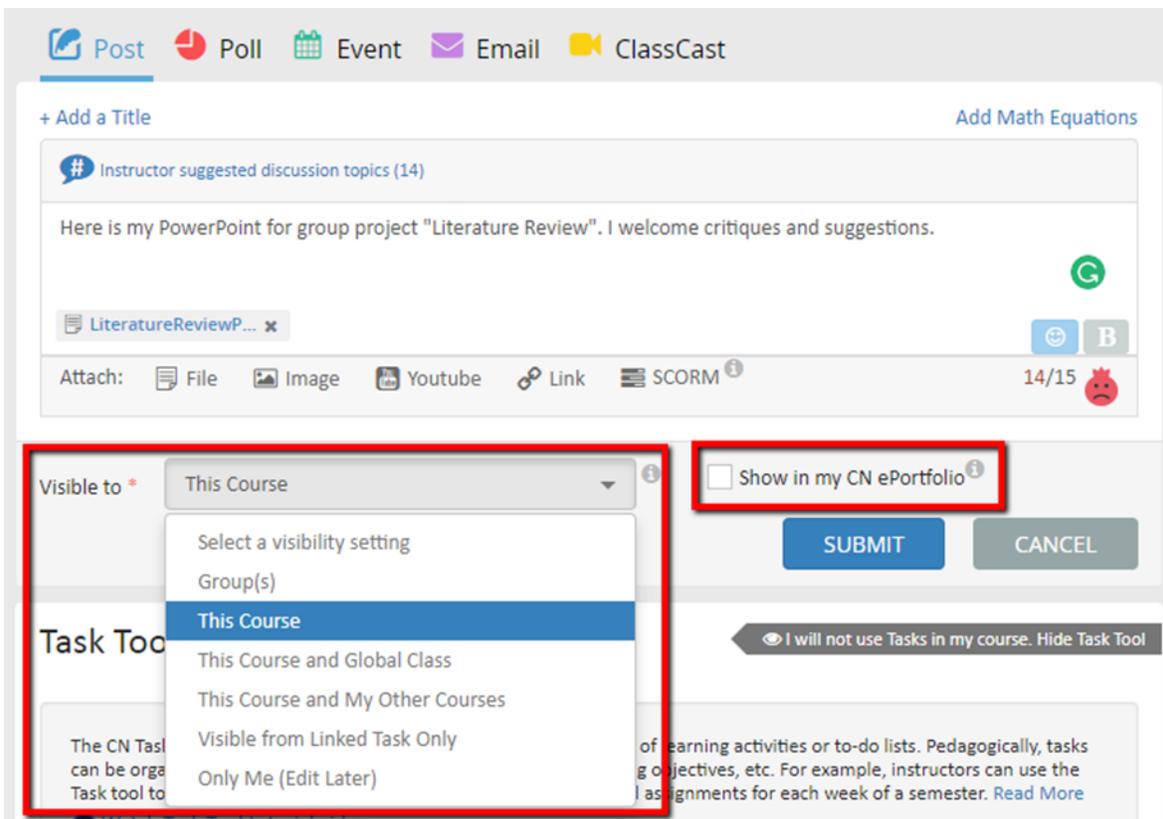
Figure 5. Post Visibility Settings

2. Course name displayed on Posts

If users are both members of the same course, they see the name of their mutual course on each other's course posts. If users are not from the same course (for example they Global Classmates), then they will not be able to see the name of the course, from which the post was created. See and compare **Figure 6** and **Figure 7**
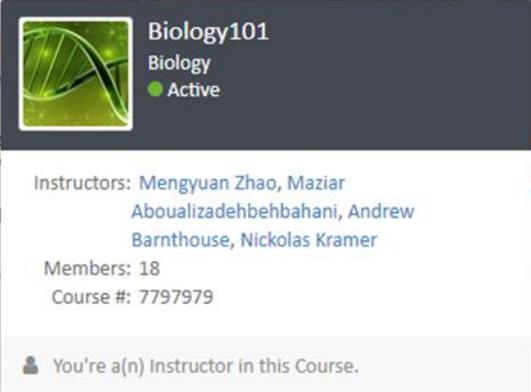
Figure 6. Members of the same course

Figure 7. Members are not in the same course; they are global classmates

Anar Seed Privacy Settings

By default, course Anar Seeds are visible to all course members, see **Figure 8**. This means students can view each other's Anar Seeds received from the course. The user who receives the most Anar Seeds at any given time is called "Anar Seeds Champion," and is also shown on the right side of the Anar Seeds Progress bar to each course member, as in **Figure 9**. If course instructors count Anar Seeds toward the course grade or have any concerns about student privacy related to Anar Seeds, they can go to course Roster from the left-hand menu on a course page, click "Anar Seeds Privacy Settings" and check one or both of the privacy options.

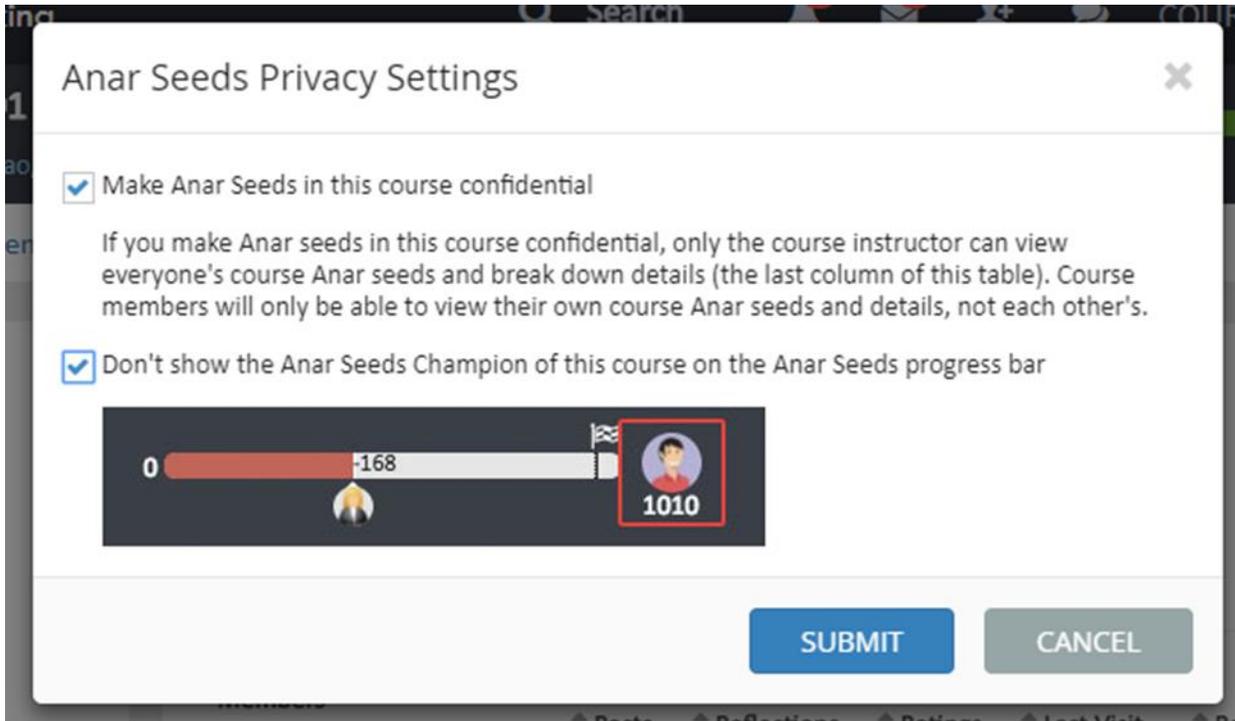**Figure 8. Anar Seed Privacy Settings**

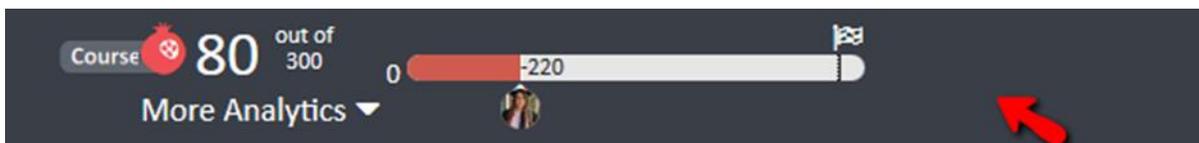**Figure 9. Make Anar Seeds Confidential**

Once done, students will not be able to view each other's Anar Seeds. They will only be able to see their own course seeds, see **Figure 10**. The Anar Seeds Champion will also be hidden from the seeds progress bar, see **Figure 11**.

Figure 10. Hide Anar Seeds in Roster

Figure 11. Hide Anar Seeds Champion

Account/ePortfolio Settings

1. Users can choose whom they want to make each piece of their profile/ePortfolio visible to, see **Figure 12**.
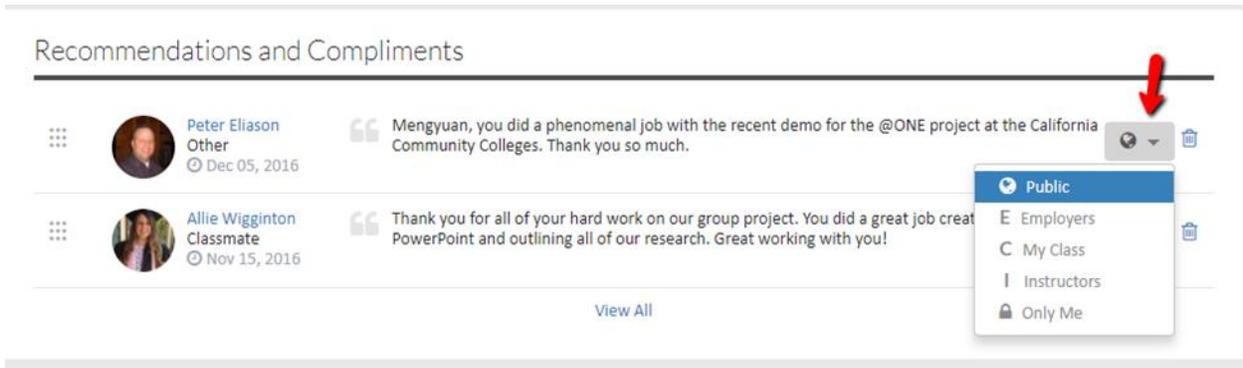
Figure 12. ePortfolio Visibility Settings

2. For badges, users can hide badges they do not want to display on their ePortfolio. For badges they do want to display on their ePortfolio, they can hide (see **Figure 14**) course-related information (name of the course from which they received the badge and Award Criteria (see **Figure 13** which may disclose their grade related information).
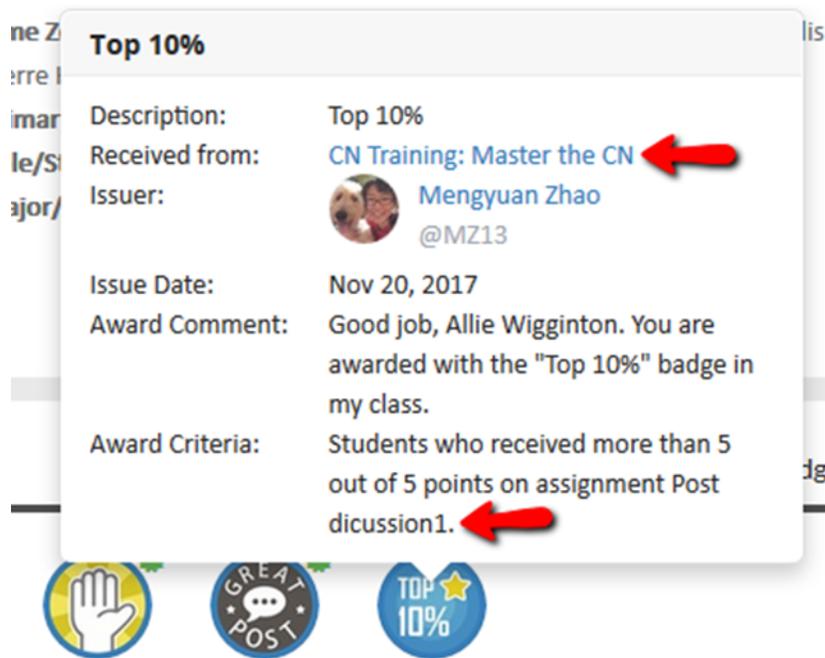

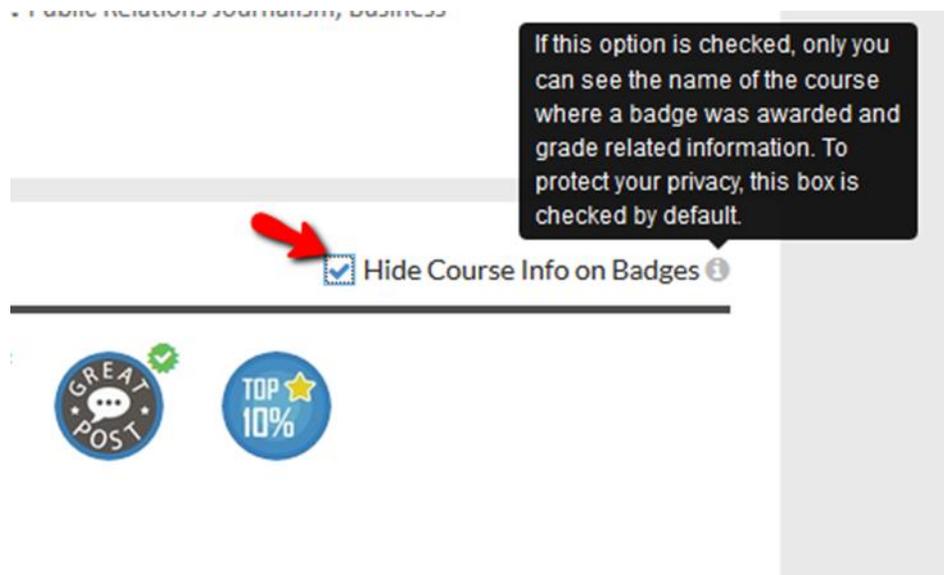**Figure 13. Default Show Course Information**

Figure 14. Hide Badge Information

After checking the "Hide Course Information on Badges" checkbox in the upper right corner of the Badges section, the course name and Award Criteria are both hidden to others. See **Figure 15**.
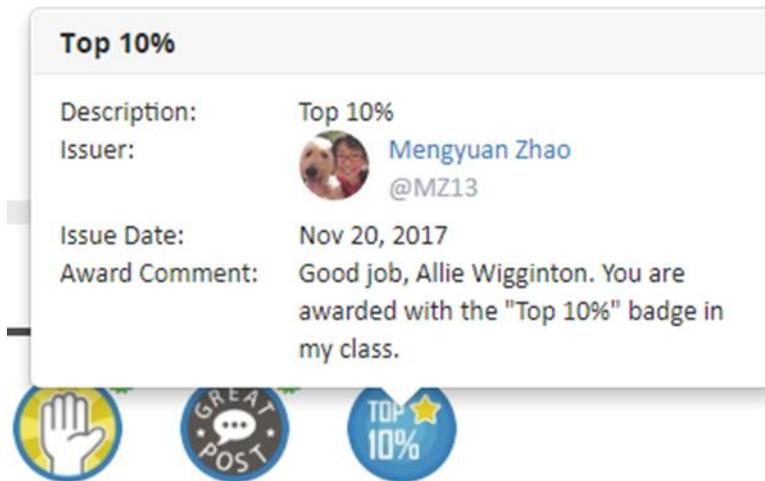

Figure 15. Hide Badge Information

3. If users do not want their ePortfolio to be viewed by the public and/or appear in Google searches and other search engines, they can click "Privacy Settings" on the top right of their ePortfolio and check "Do not make my profile visible to the public." See **Figure 16**.
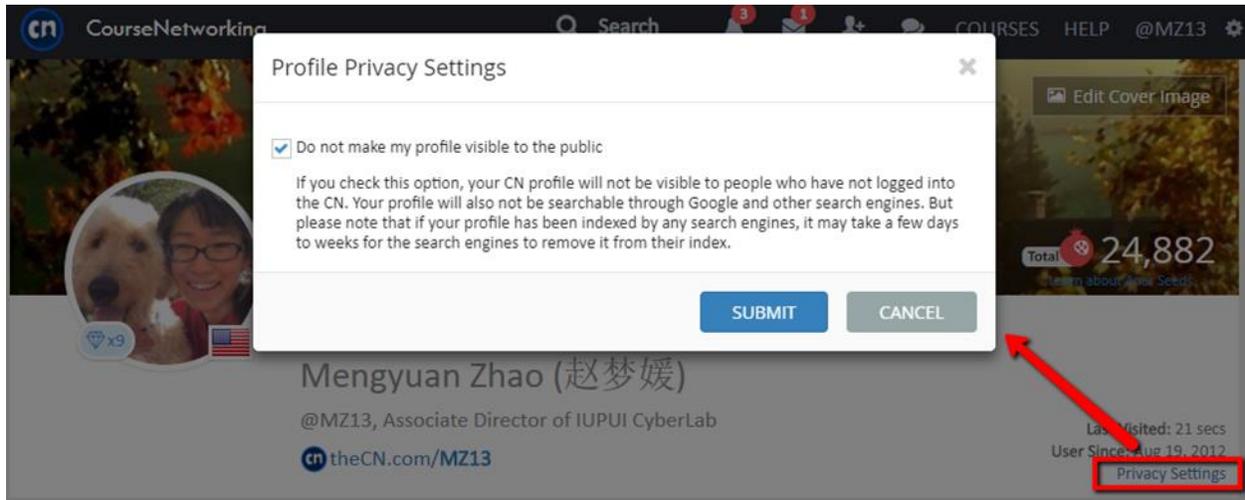
Figure 16. User ePortfolio

4. Licensed institutions (Admin) can completely disable their members' ePortfolios. If they do so, their members will not be found or viewed by any CN users. Choosing the first bubble shown in **Figure 17** below will disable anyone (even users from your own institution) from viewing the ePortfolio. Only the individual user themselves can see it. Selecting bubble two shown below will allow institutions to select labels for certain grades or groups to be hidden from the public. Only institution members to see each other's' ePortfolios of the certain groups.

Figure 17. Institution Disable Public View

Authentication Integration

Single-Sign-On (SSO) is configured at the account level. SSO gives the institution complete control over which users are authenticated and how that authentication is executed. 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.

Other Default FERPA-related features

Additional features in CourseNetworking related to FERPA compliance include:

- Names, not potentially sensitive contact information, are displayed on CourseNetworking
  - o CourseNetworking displays students' names in the course, their CN number, and chosen country. CN does not display email addresses or other information inputted by default;

however students may choose to show this information by changing the visibility settings. Users on CN may contact any other user also on CN but the communication will be mediated through CourseNetworking and users' actual contact information will not be disclosed. Institutions can disable this feature.

☑ Customize automatic logout period for inactive users (by default, CN logs out users after 30 days of inactivity)

Automatically log out user after [30] [Days ▾] of inactivity.

Figure 18. Log-off Inactive Users