TERMS AND CONDITIONS

ACCESSIBILITY
Link here

PRIVACY POLICY
Link here

TERMS OF SERVICE
Link here

Uvii is dedicated to continuously improving our websites, applications and features to create an accessible and inclusive learning environment for as many students as possible. Our products and services are designed based on the internationally recognized **Web Content Accessibility Guidelines (WCAG) 2.1 Level AA and Section 508 standards** in the United States.

To ensure and validate our accessibility compliance, a third-party vendor conducts regular audits of the Uvii platform.

Student Access- Any time. Uvii makes learning and access to curriculum available to students 24 hours a day on mobile for real-time video response learning and assessment. Uvii uses a familiar social media style interface and makes it easy for students to access course post and micro assessment q&a and surveys to give feedback and communicate directly with instructors in a siloed learning environment without relying on a personal computer/ laptop or don't need stable access to WiFi in order to respond to curriculum and stay engaged.

UVII takes User privacy seriously, and are committed to safeguarding the privacy of the Users of our Services.

New York Privacy Notice (SHIELD Act)

New York's original data breach notification law required any person or business conducting business in New York to notify state residents when their "private information" was acquired without valid authorization. *See* N.Y. Gen. Bus. L. § 899-aa(2).

The SHIELD Act, which takes effect on March 21, 2020, broadens the scope of New York's data breach notification law in several ways. The notification requirements now apply to any person and business that handles New York residents' information *regardless of whether that person or business conducts business in New York*.

New York's data breach notification law requires any person or business conducting business in New York to notify state residents when their "private information" was acquired without valid authorization. *See* N.Y. Gen. Bus. L. § 899-aa(2). The SHIELD Act, as of March 21, 2020, broadens the scope of New York's data breach notification law in several ways. The notification requirements now apply to any person and business that handles New York residents' information *regardless of whether that person or business conducts business in New York*.

SHIELD Act requires any person or business handling New York residents' private information to implement and maintain "reasonable" administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of private information. New York SHIELD Act now mandates that a covered company:

A. designate one or more employees to coordinate the security program;
B. identify reasonably foreseeable internal and external risks;
C. assess the sufficiency of safeguards in place to control the identified risks;
D. train and manage employees in the security program practices and procedures;
E. select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract;
F. adjust the security program in light of business changes or new circumstances;
G. assess risks in network and software design;
H. assess risks in information processing, transmission and storage;
I. detect, prevent and respond to attacks or system failures;
J. regularly test and monitor the effectiveness of key controls, systems and procedures;
K. assess risks of information storage and disposal;
L. detect, prevent and respond to intrusions;
M. protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and

N. dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.
O. In addition, the SHIELD Act notifications:
P. Expanded definition of "private information"
   The SHIELD Act expands "private information" in line with the laws of several other states to include (i) biometric information, (ii) financial account numbers that can be used alone to access an account, and (iii) usernames or email address in combination with a password or security question and answer.
Q. Notification for incidents involving unauthorized access
   Under the original law, notification was required only if there was "unauthorized acquisition" of private information. The SHIELD Act requires notification even where there was "unauthorized access" but no acquisition of private information, such as where consumers with the right to freeze their credit at no cost, goes into effect on September 23, 2019.

California Consumer Privacy Act ("CCPA")

Privacy Notice – California Consumer Privacy Act

This Notice details how we will treat your data when the data is subject to the California Consumer Privacy Act (CCPA).

Definitions
Under CCPA, “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

A “Consumer” is a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, including by any unique identifier.
Personal information includes, but is not limited to, the following:

A. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.
B. Any categories of personal information described in subdivision (e) of Section 1798.80.
C. Characteristics of protected classifications under California or federal law.

D. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
E. Biometric information.
F. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
G. Geolocation data.
H. Audio, electronic, visual, thermal, olfactory, or similar information.
Professional or employment-related information.
I. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
J. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
K. "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information.

What Personal Information do we collect?

We may collect, store, and use the following kinds of information and Personal Information ("Collected Information"):

Information about your account and use of the UVII Services including any transactions carried out between you and us on the platform, and information relating to any purchases you make of services.

This may include but is not limited to:

First name
Last name
Address
Date of birth
E-mail address
Country of residence
Location data
Online identifier or pseudonym, which includes IP addresses and cookie identifiers
Application usage data
Email communication data

Call recording data
Information that may be considered Personal Information when such information is combined with other information includes but is not limited to:

name of education Institution
student ID number
cell phone number
The purposes of processing Personal Information
To ensure our Users have the best experience with the platform, Personal Information, will be used for:

Allowing Users to create accounts on UVII Services
Providing Users with the ability to access, download and use all UVIIServices as defined in the Terms of Service
Providing operational services such as Account Management and Technical Support
Detecting, preventing and addressing technical issues
Assisting UVII in improving, developing and creating products, services and content to meet the needs of Users
Communicating with Users regarding security, privacy, and administrative issues relating to Users use of products and services.
Providing Institutions with educational evaluation information necessary to implement the Service
Recording student location for secure attendance
Providing information about new products, services, newsletters, informative emails, and research on future product ideas or improvements (if Users have opted-in to receive such information)
Processing payments
Sharing Collected Information
We may share Collected Information about you:

(a) to enable our third-party sub-processors to provide services including but not limited to:
payment processing
data center hosting services
database provision
dialer infrastructure services
email sync services
marketing operations services
auditing
collecting debts
fulfilling orders
(b) to the extent that we are required to do so by law;
(c) in connection with any legal proceedings or prospective legal proceedings;
(d) mergers, acquisitions, financings, or corporate reorganizations

(e) in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);
(f) in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Security of Collected Information

We will take reasonable precautions to prevent the loss, misuse, or alteration of your Personal Data. Data transmission over the Internet is inherently insecure and we cannot guarantee the security of data sent over the Internet.

We will store all the Collected Information you provide or that we collect about you on our secure servers hosted by AWS.

Our full Security Policy can be found at https://uviiapp.com/company/security/

You are responsible for keeping your passwords confidential. We will not ask you for your passwords.

Retention of Your Personal Data

We maintain information about Users for as long as we provide services to the User, and for as long as it remains necessary for the identified purposes or as required by law, which may extend beyond the termination of service (unless by prior institutional arrangement).

We may retain certain data as necessary to:

prevent fraud or future abuse,
for legitimate business purposes, such as analysis of aggregated, de-identified data,
account recovery,
or if otherwise required by law

Changes to This Notice

We may update this CCPA Notice from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

Third Party Websites

The website contains links to other websites. We are not responsible for the privacy policies of third party websites or such site operators' actions, including the collection or use of your personal data.

Access to Your Personal Data

If you use this website, upon request, we will grant you reasonable access to your personal data and allow you to correct, amend or delete information that is demonstrated to be inaccurate or incomplete.
If you are a User of the UVII Services we depend on you to update and correct your personal data to the extent necessary for the purposes for which that data was collected, such as contact

information you provide, so that we can provide you technical support services, account information notices and invoicing information.

You can update your personal data under settings and accessing “My Account.”
Full instructions for this can be found here:

Professor Account
Student Account
Your Rights
Under the CCPA You have the right to request that a business that collects personal information about You disclose the following:

The categories of personal information it has collected about You.
The categories of sources from which the personal information is collected.
The business or commercial purpose for collecting or selling personal information.
The categories of third parties with whom the business shares personal information.
The specific pieces of personal information it has collected about You.
You may contact us if you wish to exercise any of your rights in respect of your personal data processed in this website or the platform.

Contact Us
To exercise your rights, or if you have any questions about this CCPA Privacy Notice, or our treatment of your personal information, please contact us using the following means:

Call: 917 781 0914
Visit: http://www.uviiapp.com/support
Email: support@uviiapp..com

Request a virtual demo of our platform to answer your questions and set up your Uvii subscription.