Honorlock™

Honorlock Security Overview

LMS Integrations

Honorlock integrates with Canvas, D2L, Moodle, and Blackboard LMS using LTI 1.3 Standards and available REST APIs; Honorlock's Intellum integration utilizes Intellum APIs. When using Honorlock through the LTI or extension, no passwords are required to use Honorlock, the LTI integration uses single-sign-on authentication and is completely OAuth-based.

Custom Integration Solutions

Honorlock is able to get up and running quickly on any platform using Honorlock's APIs and Elements. Our developer toolkit provides the independence to implement the integration on any timeline without additional custom development. After completing the Exam Administrator Experience phase of the integration, users (admins) will be able to effectively manage and track the progress of individual exams, as well as access exam results.

Hosting Provider Overview

Honorlock is an on-demand online proctoring solution with 24/7/365 availability. Cloud-computing (SaaS) infrastructure is provided by Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (EC2), and fully redundant storage infrastructure of the Amazon Simple Storage Service (S3). Customer data is hosted by Amazon Web Services with multiple availability zones and backups are saved to another region. All data is processed and stored within the United States.

Organizational Security

A core tenet of Honorlock's security revolves around the policies and procedures we've put in place to ensure all of the Honorlock team members are protecting the data of our customers. All Honorlock employees must pass a background check and sign non-disclosure agreements prior to starting at Honorlock. They are also required to complete annual trainings on Information Security, Privacy, FERPA, Sexual Harrassment, and social engineering (including phishing). Developers participate in secure coding and general security best practices training. Beyond training, Honorlock regularly prepares for incidents and disaster recovery. Our incident response plan is focused on procedures to detect, respond to, and limit the effects of any incident. We test and confirm the success of our incident response plan and Business Continuity plans annually.

Infrastructure & Development

Honorlock takes a security-first approach in the infrastructure and development of the Honorlock application. All data is encrypted in transit and at rest using industry standard best practices. It is Honorlock's policy to follow the principle of least privilege. Privileged access must also be provisioned with the minimum amount of access possible to perform job functions and both are managed with Role-Based Access Control (RBAC). Honorlock's security monitoring ensures appropriate mechanisms are in place to secure systems and applications and are not bypassed. Additionally, Honorlock conducts routine third party vulnerability assessments, scans, and monthly penetration testing to ensure data protection.

Compliance

Soc 2 Type 2 Audit

Honorlock has achieved Soc 2 Type 2 compliance, completed by the American Institute of Certified Public Accountants (AICPA) System Organization Control (SOC) 2 Type 2 audit. Completion of the SOC 2 Type 2 audit confirms that Honorlock has the appropriate and correct system controls in place to safeguard customer data and that the system controls are operating as expected.

GDPR Compliance

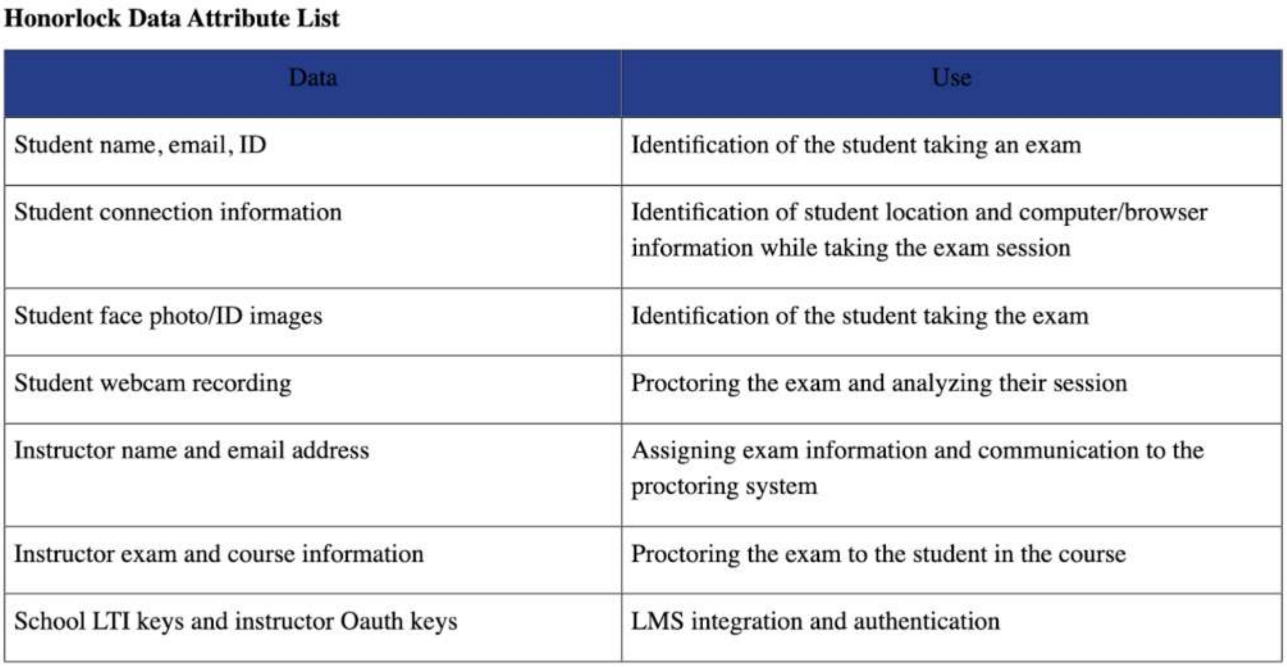
The GDPR (General Data Protection Regulation) is an EU Regulation that replaced the 1995 EU Data Protection Directive (DPD) to significantly enhance the protection of the personal data of EU citizens and increase the obligations on organizations that collect or process personal data. The regulation builds on many of the 1995 Directive's requirements for data privacy and security. but includes several new provisions to bolster the rights of data subjects and add harsher penalties for violations. We are fully committed to enhancing the Honorlock platform to enable easier compliance with the GDPR and have validated the GDPR readiness of our various services internally.

Authentication & Data

Honorlock is committed to protecting your privacy. Honorlock is not the owner of the data but does hold the data for the institution; data retention periods are established within each customer's MSA. Employees do not have access to personal data unless their job requires it (e.g. support or proctors) and all employees complete training that covers the proper handling of data. Additional information on what is collected can be found in our Student Privacy FAQ.

In order to take an exam, students are required to install the Honorlock Chrome extension. This extension requests access to read and change data on websites and capture the content of the user screen. The Honorlock extension is only active and recording information when an exam is in progress, and a visual indicator is available to notify the user that the extension is active.

Honorlock collects the following information from the LMS for students taking assessments:



Honorlock Data Attribute List

Data	Use
Student name, email, ID	Identification of the student taking an exam
Student connection information	Identification of student location and computer/browser information while taking the exam session
Student face photo/ID images	Identification of the student taking the exam
Student webcam recording	Proctoring the exam and analyzing their session
Instructor name and email address	Assigning exam information and communication to the proctoring system
Instructor exam and course information	Proctoring the exam to the student in the course
School LTI keys and instructor Oauth keys	LMS integration and authentication

Honorlock™

Honorlock.com
+1 (844) 243-2500

Honorlock™

phone: +1 844-243-2500
email: support@honorlock.com

Last Updated: August 2023