Background

Student privacy when recording video and audio of a user is taken seriously to ensure Honorlock does everything it can, proactively, to protect each student.

Policy Statement

Honorlock is committed to establishing policies, processes, procedures, and other safeguards to protect its vital business information throughout its lifecycle. All Honorlock information is considered *Confidential* unless it has been made available in the public domain by an authorized employee or agent. Every employee must be aware of the requirements of this policy, especially as it pertains to the custodial responsibility Honorlock has for safeguarding client information.

Scope

This policy applies to all Honorlock employees, business operations, infrastructure and information that drive the business mission. The policy covers business information in all forms that include written, verbal, and digital or any other means of conveyance. Several other Honorlock policies address controls that safeguard information and work in conjunction with this policy. The policy recognizes that certain security safeguards that protect Honorlock information are not intended to cover all aspects of protection of data.

This policy applies to:

- Systems belonging to, or under the control of, Honorlock;
- Information stored, or in use, on Honorlock systems;
- Information in transit across Honorlock' voice or data networks;
- Control of information leaving Honorlock;
- Information access resources;
- All parties who have access to, or use of systems and information belonging to, or under the control of, Honorlock including Honorlock employees, Contractors, Vendors/Other Third Party, Customers, any other party utilizing Honorlock resources

Application of this policy applies throughout the information lifecycle from acquisition/creation, through to utilization, storage, and disposal.

Goals

It is the goal of the Honorlock Student Privacy & Proctoring Guidelines related to Privacy Incidents to protect student privacy. This is achieved by:

- Provide direction and support for student privacy in accordance with business requirements, regulations and legal requirements;
- State the responsibilities of staff, partners, contractors and any other individual or organization having access to Honorlock systems;
- State management intent to support the goals and principles of student privacy in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity, and availability of resources can be maintained.
- Optimize the management of risks, by preventing and minimizing the impact of student privacy;
- Ensure that all incidents of student privacy are reported, investigated and appropriate action is taken where required;
- Ensure student privacy requirements are regularly communicated to all relevant parties.

Principles

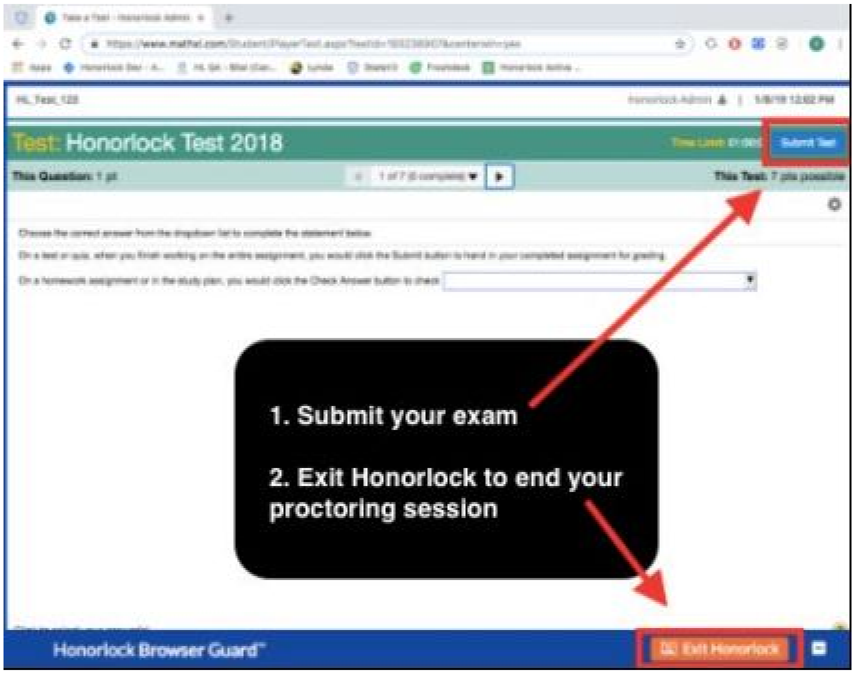
Honorlock will establish proactive measures to ensure student privacy is upheld in situations identified that can create accidental sharing of video or audio

Exam Recordings

- Honorlock provides users with a visual representation when recording is live, indicated by a red flashing badge displayed on the Honorlock Chrome Extension. This is to ensure that a user is always aware of an in-progress recording taking place.

Example:

- Honorlock identifies when a student exam ends. This is determined by the student submitting an exam within their LMS. When this occurs, Honorlock automatically stops all recording and ends the exam session being monitored by Honorlock. This ends the recording of the webcam, the desktop screen, and the audio.
- For Universal Proctoring, in which exams are given outside of the LMS through a 3rd party site, Honorlock cannot detect when the exam ends to auto end a recorded session. Honorlock added UI elements for these exams that appear as a wrapped banner around the testing screen which tells the student they are in an exam in addition to the Chrome Extension Badge. When a student submits his or her exam, there is an orange Exit Honorlock Icon reminding the student to end the session.



Choose the correct answer from the dropdown list to complete the statement below.

On a test or quiz, when you finish working on the entire assignment, you would click the Submit button to hand in your completed assignment for grading.

On a homework assignment or in the study plan, you would click the Check Answer button to check

1. Submit your exam

2. Exit Honorlock to end your proctoring session

Exam Proctoring

- Honorlock provides three levels of service for proctoring which are Automated, Auto + Live Pop-In, or Manual Review. There are scenarios for all proctoring levels of services that can impact student privacy.
  - **Automated Proctoring**
    - Recording of sensitive information, which is not detected by AI, can be reported by a customer support member, a user, or a faculty member who

    reviews the session. Honorlock has implemented the following practices for each scenario to ensure student privacy is maintained for this type of content. Automated Proctoring has the biggest gap in sensitive information going undetected. These incidents are usually self-reported or caught only when a session is reviewed.

        - Support members providing support to a student testing may need to do a screen share or view the session live through the Honorlock proctoring application. During this time it is possible that confidential information is detected on the users desktop recording (bank info, credit card info, username passwords, etc). It is also possible that accidental nudity of the user occurs. When sensitive information like this is witnessed, it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will notify the faculty member who owns the exam to provide them with an update about the incident and to report that the content has been removed for student privacy reasons.
        - A user taking an exam can accidentally reveal sensitive information. When this occurs and a student contacts Honorlock to report the incident such as realizing they had sensitive information present on their desktop being recorded, accidentally submitting a Social Security Card in lieu of a student ID, knowing they committed an act of accidental nudity, etc. it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will notify the faculty member who owns the exam to provide them with an update about the incident and to report that the content has been removed for student privacy reasons.
        - A faculty member reviewing a student session can identify sensitive information as part of their review. When this occurs and a faculty member contacts Honorlock to report the incident that confidential information is detected on the users desktop recording (bank info, credit card info, username passwords, etc) or accidental nudity of the user occurs it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will follow up with the faculty member who reported the incident to notify them the content has been removed from the session.

- **Automated Proctoring + Live Pop-In**
    - Recording of sensitive information can be detected by a customer support member or proctors when interacting with students actively taking exams.

Honorlock has implemented the following practices to ensure student privacy is maintained for this type of content.

- Support members providing support to a student testing may need to do a screen share or view the session live through the Honorlock proctoring application. During this time it is possible that confidential information is detected on the users desktop recording (bank info, credit card info, username passwords, etc). It is also possible that accidental nudity of the user occurs. When sensitive information like this is witnessed, it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will notify the faculty member who owns the exam to provide them with an update about the incident and to report that the content has been removed for student privacy reasons.
- If a proctor is alerted to an exam session, he or she may join an active session with a user. If during that time any sensitive information is revealed or witnessed, the proctor will report the incident to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will follow up with the faculty member who reported the incident to notify them the content has been removed from the session.
- Because proctors are not joining all sessions, and when they do, the sessions are not reviewed in their entirety, there is a gap in which proctors would not detect the sensitive information. Due to this void, a user taking an exam who accidentally reveals sensitive information can still contact Honorlock to report the incident such as realizing they had sensitive information present on their desktop being recorded, accidentally submitting a Social Security Card in lieu of a student ID, knowing they committed an act of accidental nudity, etc. it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will notify the faculty member who owns the exam to provide them with an update about the incident and to report that the content has been removed for student privacy reasons.
- A faculty member reviewing a student session can identify sensitive information as part of their review. When this occurs and a faculty member contacts Honorlock to report the incident that confidential information is detected on the users desktop recording (bank info, credit card info, username passwords, etc) or accidental nudity of the user occurs it is reported by the support member to management.

Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will follow up with the faculty member who reported the incident to notify them the content has been removed from the session.

- **Manual Review**
    - Recording of sensitive information has the highest chance of being seen by a manual review proctor than any other level of service. Proctors are reviewing the entire session from start to end. This review is done at a rate of 2-4x based on the experience of the proctor as well as how detailed the guidelines provided dictate, so there is still a chance that sensitive information could be missed depending on the duration present on the screen. Honorlock has implemented the following practices to ensure student privacy is maintained for this type of content when using our manual review level of service.
        - Support members providing support to a student testing may need to do a screen share or view the session live through the Honorlock proctoring application. During this time it is possible that confidential information is detected on the users desktop recording (bank info, credit card info, username passwords, etc). It is also possible that accidental nudity of the user occurs. When sensitive information like this is witnessed, it is reported by the support member to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will notify the faculty member who owns the exam to provide them with an update about the incident and to report that the content has been removed for student privacy reasons.
        - When a proctor reviewing an entire student session identifies sensitive information that is revealed, the proctor will report the incident to management. Management will create an incident, submit a ticket to development, and the sensitive information will be scrubbed from the video. Once this is completed, the Customer Success Manager for the account will follow up with the faculty member who reported the incident to notify them the content has been removed from the session.

Incident Report

- When an incident occurs, containing student sensitive information, management will be required to complete the following steps:
    - Create an incident form to document the incident. The report will document the institution, student name, exam or session info, and a description of what occurred.
    - Create a google doc and share only with VP, Customer Success to disseminate to parties who will take action to remedy the content.

- Create and submit a Jira ticket to the development team. The Jira ticket will not contain the details or directly link to the content but will link only to the protected google doc so that others within the company have no direct way to access the content
- Notify the VP, Customer Success of the Incident and provide the Jira ticket and google doc information needed to proceed with the remedy
- The VP, Customer Success will confer with the CTO, who will assign the ticket to a developer who will then be granted access to the content for scrubbing and/or removal. Once completed, the developer will document his or her actions taken in the Jira ticket.
- The VP, Customer Success will then notify the CSM of the account the incident occurred and was remedied and authorize client communication.

Data Handling/Scrubbing/Retention

- Depending on the content of the recording, a decision to scrub, filter out, or delete will be made by the CTO and VP, Customer Success after review.
    - Things that will be considered include but are not limited to:
        - Can the content be used to take action against academic dishonesty?
        - Does the content add value to the overall documentation of student success or academic dishonesty? (visual proof of cheating such as a cell phone being used while exposure of nudity is present in the video simultaneously)
        - Does the safety of the student outweigh the benefit? (disclosure of SSN, Bank Account Info, etc)
        - Does the recording infringe on the privacy of the student?
        - Can Honorlock make a copy of the original video for storage (in the event it is necessary for use), but edit the content viewable by faculty to protect the student?
        - Does audio-only achieve proof of academic dishonesty as a stand-alone without the compromising video accompanying the audio? (Nudity on screen adding no value, but the conversation occurring at the time discloses cheating)
        - Is the user a minor? (child protection laws)
        - Was the incident intentional or accidental?
    - Once a decision is made, the developer will take the instruction provided to delete, edit, or scrub the video.
        - In the event that a decision is made to delete a record, a copy will be made and retained for 6 months as stated in our MSA
        - In the event of editing or scrubbing video which alters the original content, there will not be a second copy or original retained. Editing consists of blurring the area containing the sensitive information and for that reason, there is not a need to retain an original copy.

Client Communication

- Client communication will happen within 24 business hours of an incident occurring and being reported internally.
- The communication will be provided to the faculty member owning the exam in which the content occurred.
- The communication will be provided by the Customer Success Manager assigned to the account. The VP, Customer Success will accompany the CSM if requested.
- Communication will include:
    - The reason for the call
    - The exam in which the incident occurred
    - The date of the incident
    - The student of who the exam session is affiliated with
    - The type of sensitive information involved
    - The method in which the incident was identified (student reported, proctoring found, etc)
    - The resolution (what was deleted, edited, etc)
    - The current status of the content (original kept, edited version present in session viewer, etc)
    - Ensure there are no questions or concerns from the faculty member
    - A reminder that data is stored for 6 months per HL retention policy
- The CSM will then conclude the communication with updating the VP, Customer Success.