- **Terms & Privacy**
- **GDPR**
- **Trademark**
- **Security**
- **Cookie Policy**
- **Google Data Use Disclosure**

# Terms & Privacy

**Effective Date:** May 19, 2025

This document constitutes the Terms of Service ("Agreement") and Privacy Policy for HonTru LLC, governing the use of our web and mobile software services, including Mentor AI and School AI applications (collectively, the "Services"). These terms apply to all users, including individuals, educational institutions, educators, students, and other entities. By accessing or using the Services, you agree to be bound by this Agreement. If you do not agree, you must not use the Services.

**1. Introduction**
This Agreement is a legally binding contract between you (an individual, educational institution, or other entity) and HonTru LLC, a company dedicated to fostering collaborative learning and mentorship. Our Services include Mentor AI and School AI, web and mobile applications designed to provide AI-driven tutoring, collaborative learning environments, and mentorship programs for educational and professional purposes. This Agreement governs your access to and use of the Services, including any updates, features, or content provided by HonTru LLC. If you represent an organization, such as a school or company, you warrant that you have the authority to bind that organization to these terms.

**2. Acceptance of Terms**
By accessing or using the Services, including Mentor AI, School AI, or any related platforms, you agree to be bound by this Agreement, including the Privacy Policy and, for educational users, the Student Data Privacy Addendum. Individuals must be at least 18 years old or have parental/guardian consent if under 18, as required by the Children’s Online Privacy Protection Act (COPPA) or other applicable laws. If acting on behalf of an organization, you represent that you have the authority to bind that organization. If you do not agree to these terms or lack authority, you must not use the Services. HonTru LLC may update this Agreement periodically, notifying users via our website (https://www.hontru.com/) or email. Continued use after updates constitutes acceptance of the revised terms.

**3. Definitions**
For clarity, the following terms are defined as used in this Agreement:

- **Services**: Web and mobile software provided by HonTru LLC, including Mentor AI, School AI, and related platforms like HonTru AIStudent for educational use.
- **Content**: All materials available through the Services, including text, images, videos, and

AI-generated outputs.

- **Data**: Information provided by users to access or use the Services, including personal and educational data.
- **User**: Any individual or entity using the Services, including Educators, Students, and Educational Institutions.
- **Educator**: An individual at least 18 years old, employed by or affiliated with an Educational Institution, authorized to use the Services on its behalf.
- **Student**: An individual, typically under 18, enrolled in or associated with an Educational Institution, using Student-Facing Services.
- **Educational Institution**: A school, college, university, or other entity providing education to Students.
- **Student Data**: Personally identifiable information about a Student, such as names, email addresses, academic records, or usage data.
- **Student-Facing Services**: Services designed for Students, such as HonTru AIStudent, with enhanced privacy protections.

**4. License Grant**

HonTru LLC grants you a non-exclusive, non-transferable, non-sublicensable license to use the Services for your internal business operations or, for Educational Institutions, educational purposes, in accordance with this Agreement and any provided documentation. This license includes access to Content and features like AI tutors and collaborative rooms, subject to compliance with these terms. You may not modify, distribute, or create derivative works from the Services without prior written consent from HonTru LLC.

**5. User Responsibilities**

You agree to use the Services responsibly and in compliance with all applicable laws, including privacy and intellectual property laws. Your responsibilities include:

- Maintaining the security of your account credentials and notifying HonTru LLC of any unauthorized access.
- Providing accurate and lawful Data when using the Services.
- Not using the Services to violate others' rights, engage in illegal activities, or transmit harmful content.
- Not attempting to reverse engineer, hack, or interfere with the Services' functionality.
- For Educators, reviewing AI-generated Content for accuracy and appropriateness before sharing with Students.

Failure to comply may result in suspension or termination of your access.

**6. Ownership**

- **Your Data**: You retain ownership of Data you provide, granting HonTru LLC a worldwide, non-exclusive license to use, process, and store it solely to provide the Services, improve functionality, or comply with legal obligations.
- **HonTru LLC Property**: HonTru LLC owns all rights to the Services, Content, technology, and intellectual property, including AI algorithms and software.
- **Feedback**: Suggestions or feedback you provide become HonTru LLC's property, and we may use them without compensation or attribution.
- **Student Data**: For Educational Institutions, Student Data is owned and controlled by the institution, as detailed in the Student Data Privacy Addendum.

**7. Payment**
For paid Services, you agree to pay fees as outlined on our pricing page (https://shandysystems.com/pricing.html). Fees are based on the number of administrators/mentors and include a 15% platform fee for payment processing via partners like Stripe. Billing occurs monthly, and fees are non-cancelable and nonrefundable. Late payments may result in account suspension or termination. HonTru LLC may adjust pricing with 30 days' notice, and continued use constitutes acceptance of new rates.

**8. Term and Termination**
- **Term**: This Agreement begins upon your acceptance (e.g., accessing the Services) and continues until terminated by either party.
- **Termination by You**: You may terminate your account at any time via the Services or by contacting us at admin@hontru.com.
- **Termination by HonTru LLC**: We may suspend or terminate your access for material breaches (e.g., non-payment, violation of terms) or other reasons, with 30 days' written notice unless immediate action is required.
- **Post-Termination**: Upon termination, you may access your Data for 90 days (read-only). Student Data will be handled per the Student Data Privacy Addendum. HonTru LLC is not liable for Data loss post-termination.

**9. Warranty and Liability**
The Services are provided "as is" without warranties, except as expressly stated. HonTru LLC does not guarantee uninterrupted access, error-free operation, or specific results. Our liability is limited to the fees you paid in the 12 months prior to a claim, excluding indirect, consequential, or punitive damages, except in cases of gross negligence or willful misconduct. For Educational Institutions, additional warranties regarding Student Data are provided in the Student Data Privacy Addendum.

**10. Indemnity**
- **Your Indemnity**: You agree to indemnify HonTru LLC, its affiliates, and employees against claims arising from your misuse of the Services, violation of this Agreement, or infringement of third-party rights.
- **HonTru LLC Indemnity**: We will indemnify you against claims that the Services infringe third-party intellectual property rights, provided you notify us promptly and cooperate in the defense. This does not apply to misuse or unauthorized modifications.

**11. Confidentiality**
Both parties agree to protect confidential information (e.g., business plans, user Data, Service details) and not disclose it to third parties without consent, except as required by law. For Student Data, additional protections are outlined in the Student Data Privacy Addendum. Confidential information excludes data that is publicly available, independently developed, or rightfully received from another source.

**12. Additional Terms for Educational Institutions**
These terms apply to Educational Institutions, Educators, and Students using the Services, particularly Student-Facing Services like HonTru School AI Student.

**12.1 Definitions**
See Section 3 for relevant definitions (e.g., Educator, Student, Student Data, Educational

Institution, Student-Facing Services).

**12.2 Services for Educational Institutions**
The Services provide tools for Educators (e.g., AI tutors, collaborative platforms) and Students (e.g., personalized learning via HonTru AI Student). These are designed to support educational goals, subject to this Agreement and the Student Data Privacy Addendum.

**12.3 Student Data Privacy Addendum**
This Addendum governs the collection, use, and protection of Student Data, ensuring compliance with the Family Educational Rights and Privacy Act (FERPA), COPPA, General Data Protection Regulation (GDPR) for EU users, and state laws like California's Student Online Personal Information Protection Act (SOPIPA).

**12.3.1 Data Collection**
HonTru LLC collects Student Data only as authorized by the Educational Institution, including:

- Names, student IDs, or other identifiers.
- Academic records or performance metrics.
- Communications within the platform.
- Usage data to improve Services.

**12.3.2 Data Ownership and Control**
Student Data is owned and controlled by the Educational Institution. HonTru LLC acts as a "school official" under FERPA, processing data solely under the institution's direction.

**12.3.3 Use of Student Data**
Student Data is used only for:

- Providing educational Services (e.g., personalized tutoring).
- Improving platform functionality.
- Complying with legal obligations. It is not used for targeted advertising, profiling, or non-educational purposes.

**12.3.4 Data Sharing and Disclosure**
Student Data may be shared with:

- Authorized personnel within the Educational Institution (e.g., teachers).
- Trusted service providers under confidentiality agreements.
- As required by law or with institutional consent. In case of a merger or acquisition, HonTru LLC will notify the institution and provide an opt-out option before transferring Student Data.

**12.3.5 Data Security**
HonTru LLC employs industry-standard measures, including:

- AES-256 encryption for data at rest.
- Transport Layer Security (TLS) for data in transit.
- Role-based access controls and regular security audits. In case of a data breach, we will notify the Educational Institution within 72 hours, per web:2, and follow our Data Breach Response Checklist (web:0).

**12.3.6 Data Retention and Deletion**
Student Data is retained only as long as necessary to provide the Services or meet legal

requirements. Upon termination or institutional request, we will delete or de-identify Student Data within 60 days, unless otherwise required by law.

**12.3.7 Access Rights**
Parents and eligible Students (18 or older) may access, correct, or delete Student Data by contacting the Educational Institution, which will coordinate with HonTru LLC. Requests will be processed within 45 days, or sooner if required by state law.

**12.3.8 Compliance with Laws**
HonTru LLC complies with FERPA, COPPA (relying on institutions for parental consent for students under 13), GDPR, and state laws.

**12.3.9 Indemnification**
HonTru LLC will indemnify the Educational Institution against claims arising from our breach of this Addendum or failure to comply with privacy laws, covering reasonable legal fees and damages.

**12.3.10 Warranty**
We warrant compliance with all applicable privacy laws, including FERPA, COPPA, GDPR, and state regulations, in handling Student Data.

**12.4 Responsibilities of Educators**
Educators must:

- Review AI-generated Content for accuracy, appropriateness, and bias before sharing with Students.
- Safeguard Student Data, entering personally identifiable information only as permitted by a data privacy agreement.
- Comply with institutional policies and applicable laws.

**12.5 Prohibited Uses**
In addition to general prohibitions (Section 5), Educational Institutions, Educators, and Students must not:

- Collect or process Student Data in violation of laws or policies.
- Share Student Data with unauthorized parties.
- Use the Services to harm or exploit Students.

**12.6 Termination**
Termination follows Section 8, with Student Data handled per this Addendum (e.g., deletion within 60 days).

**13. Privacy Policy**
This Privacy Policy governs the collection, use, and protection of personal information, with Student Data covered by the Student Data Privacy Addendum.

**13.1 Information We Collect**
We collect:

- Personal information (e.g., names, email addresses) provided by users.
- Usage data (e.g., interactions with the Services) to improve functionality.
- For Educational Institutions, Student Data as defined in Section 3.

**13.2 Use of Information**
We use information to:
- Provide and enhance the Services.
- Communicate with users (e.g., updates, support).
- Comply with legal obligations. Student Data is used solely for educational purposes, per Section 12.3.3.

**13.3 Sharing of Information**
We share information with:
- Service providers under confidentiality agreements.
- As required by law or with user consent.
- For Educational Institutions, as permitted by the Student Data Privacy Addendum.

**13.4 Data Security**
We use industry-standard security measures (e.g., encryption, access controls). However, no method is 100% secure. Student Data security is detailed in Section 12.3.5.

**13.5 Your Choices**
You may access, correct, or delete your personal information by contacting admin@hontru.com. For Student Data, contact your Educational Institution.

**13.6 Changes to this Policy**
We may update this Privacy Policy, notifying users via our website or email. Continued use after updates constitutes acceptance.

**14. Governing Law**
This Agreement is governed by the laws of the State of Colorado, excluding conflict-of-law principles. Any disputes will be resolved in state or federal courts in Boulder, Colorado, and you consent to their jurisdiction.

**15. Miscellaneous**
- **Entire Agreement**: This Agreement, including referenced policies, is the complete agreement between you and HonTru LLC, superseding prior agreements.
- **Severability**: If any provision is unenforceable, the remaining provisions remain in effect.
- **Assignment**: You may not assign this Agreement without our consent. HonTru LLC may assign it in connection with a merger or acquisition.
- **Force Majeure**: Neither party is liable for delays due to events beyond their control (e.g., natural disasters).

**16. Contact Us**
For questions, contact:
- **Email**: admin@hontru.com

For Student Data inquiries, parents and Students should contact their Educational Institution.

# General Data Protection Regulation (GDPR)

**1. Introduction**
This DPA establishes the data protection, security, and confidentiality obligations for the Processing of Personal Data collected, stored, or otherwise processed by HonTru LLC to provide the Services. It applies to you (the "Data Controller") and HonTru LLC (the "Data Processor") when you use the Services under GDPR's scope. This DPA is entered into by HonTru LLC, located at [Your Address], Boulder, CO, and you, the legal entity corresponding to your HonTru LLC Account. Collectively, you and HonTru LLC are the "Parties."

**1.1 Acceptance**
To accept this DPA, you must:

- Have an active HonTru LLC Account or be authorized to create one.
- Click the "I Accept" button on the HonTru LLC website or Services interface. Upon receipt of your time-stamped acceptance, this DPA becomes legally binding. If you lack an Account or authority to bind your entity, any attempt to accept this DPA is void.

**2. Definitions**
Capitalized terms not defined here have the meanings given in the Agreement. For this DPA:

- **Applicable Law**: Includes the GDPR, EU Directive 2002/58/EC ("e-Privacy Directive"), EU Member State laws supplementing GDPR or implementing the e-Privacy Directive (e.g., regulating cookies, unsolicited communications), security breach notification laws, and the Payment Card Industry Data Security Standards (PCI DSS).
- **Data Controller**: The entity that determines the purposes and means of Processing Personal Data, typically you, the user of the Services.
- **Data Processor**: The entity that Processes Personal Data on behalf of the Data Controller, here HonTru LLC.
- **Data Subject**: An identified or identifiable natural person whose Personal Data is processed.
- **Instructions**: This DPA and any written agreement or documentation from the Data Controller directing HonTru LLC to perform specific Processing of Personal Data.
- **Personal Data**: Information relating to an identifiable natural person, such as name, identification number, location data, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity, processed by HonTru LLC to provide the Services.
- **Processing**: Any operation on Personal Data, including collection, storage, organization, use, disclosure, combination, restriction, erasure, or destruction.
- **Pseudonymization**: Processing Personal Data so it cannot be attributed to a Data Subject without additional information, kept separately.
- **Sensitive Data**: Personal Data revealing racial/ethnic origins, political opinions, religious beliefs, trade union membership, genetic/biometric data, health, or sex life/orientation.
- **Sub-processor**: An entity engaged by HonTru LLC to Process Personal Data on behalf of the Data Controller.
- **Supervisory Authority**: An independent public authority established under GDPR to monitor data protection compliance.

**3. Roles and Responsibilities**

**3.1 HonTru LLC as Data Processor**
When providing Services like Mentor AI and School AI, HonTru LLC acts as a Data Processor, Processing Personal Data on your behalf as the Data Controller. This includes managing user accounts, delivering AI-driven tutoring, and facilitating collaborative learning environments. HonTru LLC will:

- Process Personal Data only according to your documented Instructions and this DPA,

unless required otherwise by Applicable Law (notifying you if feasible).
- Ensure personnel authorized to Process Personal Data are bound by confidentiality obligations.
- Implement technical and organizational measures to protect Personal Data, as detailed in Section 6.
- Engage Sub-processors per Section 5, ensuring equivalent data protection obligations.

**3.2 Data Controller Responsibilities**
As the Data Controller, you agree to:
- Process Personal Data in compliance with Applicable Law, providing lawful Instructions to HonTru LLC.
- Inform Data Subjects about the Processing of their Personal Data, obtaining consent where required (e.g., for students under 16 per GDPR Article 8).
- Ensure the accuracy and lawfulness of Personal Data provided to HonTru LLC.
- Respond to Data Subject requests, with assistance from HonTru LLC as outlined in Section 4.

**3.3 HonTru LLC as Data Controller**
In limited cases (e.g., processing user account information for service administration or analytics), HonTru LLC may act as a Data Controller. Such processing is governed by the Agreement's Privacy Policy, not this DPA.

**3.4 Details of Processing**
The subject matter, duration, nature, purpose, types of Personal Data, and categories of Data Subjects are specified in **Schedule A** below.

**4. Data Subject Rights**

**4.1 Handling Requests**
HonTru LLC will promptly notify you of any Data Subject requests to access, correct, erase, restrict, or object to Processing, or to exercise data portability rights, unless prohibited by Applicable Law. HonTru LLC will not respond to such requests without your written Instructions, except as required by law.

**4.2 Assistance**
Upon your request, HonTru LLC will provide reasonable assistance to fulfill Data Subject requests, including technical measures to facilitate access or deletion. You are responsible for costs associated with this assistance, unless otherwise agreed.

**5. Sub-processors**

**5.1 Authorization**
You grant HonTru LLC general written authorization to engage Sub-processors to Process Personal Data as necessary to provide the Services. This includes HonTru LLC affiliates and third-party providers (e.g., cloud hosting, analytics services).

**5.2 Sub-processor Obligations**
HonTru LLC will:
- Enter into written agreements with Sub-processors imposing data protection obligations at least as restrictive as those in this DPA.
- Remain liable for Sub-processors' compliance with these obligations, except as limited by the Agreement.
- Provide a list of current Sub-processors upon request, available by contacting admin@hontru.com.

**5.3 Notification and Objection**
HonTru LLC will notify you of new Sub-processors via email or the Services interface at least 14 days before they Process Personal Data. You may object on reasonable, legitimate grounds (e.g., data protection concerns) within 10 days of notice. If you object:

- HonTru LLC will work to address your concerns or propose alternatives.
- If no resolution is reached, you may terminate the affected Services per the Agreement's termination terms, acknowledging that Sub-processors are essential to Service delivery.

**6. Security Measures**

**6.1 Technical and Organizational Measures**
HonTru LLC will implement and maintain appropriate measures to ensure the security, confidentiality, and integrity of Personal Data, including:

- **Pseudonymization and Encryption**: Using AES-256 encryption for data at rest and TLS for data in transit.
- **Access Controls**: Role-based access, multi-factor authentication, and regular access reviews.
- **System Resilience**: Measures to ensure ongoing availability and disaster recovery, including backups and redundancy.
- **Testing and Evaluation**: Annual security audits and penetration testing to assess effectiveness.

**6.2 Incident Management**
HonTru LLC maintains a data security incident management program compliant with GDPR Article 33. If HonTru LLC becomes aware of a Personal Data Breach (e.g., unauthorized access, loss, or disclosure), it will:

- Notify you without undue delay, and no later than 72 hours after discovery, unless prohibited by law.
- Provide details of the breach's nature, likely consequences, and mitigation measures.
- Cooperate with you to investigate and remediate the breach, per GDPR requirements.

**6.3 Assistance**
HonTru LLC will assist you, at your expense, with:

- Conducting data protection impact assessments (DPIAs) per GDPR Article 35.
- Consulting Supervisory Authorities, where required.
- Fulfilling breach notification obligations to Supervisory Authorities and Data Subjects.

**7. Data Transfers**
HonTru LLC may transfer Personal Data outside the European Economic Area (EEA) or Switzerland to provide the Services. For transfers to jurisdictions without an EU adequacy decision, HonTru LLC will:

- Implement appropriate safeguards, such as Standard Contractual Clauses (SCCs) approved by the European Commission.
- Ensure Sub-processors involved in transfers comply with equivalent safeguards.
- Notify you of transfer mechanisms upon request, via admin@hontru.com.

**8. Audits and Inspections**

**8.1 Audit Rights**
You may audit HonTru LLC's compliance with this DPA once per year, or more frequently if required by Applicable Law or a Supervisory Authority. Audits must:

- Be conducted at your expense, with reasonable notice (at least 30 days).
- Occur during normal business hours, minimizing disruption.
- Be subject to a mutually agreed non-disclosure agreement.

### 8.2 Audit Support
HonTru LLC will provide access to relevant documentation, audit reports, or certifications (e.g., ISO 27001, if applicable) to demonstrate compliance. If an on-site audit is required, HonTru LLC will cooperate, subject to reasonable scope and confidentiality terms.

## 9. Return and Deletion of Personal Data
Upon termination of the Services or your request, HonTru LLC will, within 60 days:
- Return all Personal Data to you in a secure, structured format, if feasible.
- Delete all Personal Data and existing copies, unless storage is required by Applicable Law (e.g., for legal retention periods). HonTru LLC will confirm completion of deletion in writing, unless prohibited by law.

## 10. Termination
This DPA remains in effect for the duration of the Agreement and terminates concurrently with it. Obligations regarding Personal Data security, return, and deletion survive termination until all Personal Data is deleted or returned. In case of conflict between this DPA and the Agreement, this DPA prevails regarding GDPR-related Processing.

## 11. Limitation of Liability
Liability arising from this DPA, whether in contract, tort, or otherwise, is subject to the “Warranty and Liability” section of the Agreement. The aggregate liability of each Party and its affiliates under this DPA and the Agreement is limited to the fees paid by you in the 12 months prior to the claim, excluding indirect or consequential damages.

## 12. Governing Law and Dispute Resolution
This DPA is governed by the laws of Ireland, without regard to conflict-of-law principles. Any disputes arising from this DPA will be resolved in the courts of Dublin, Ireland, and you consent to their jurisdiction. The Parties will first attempt to resolve disputes through good-faith negotiation.

## 13. Contact Information
For questions about this DPA or GDPR compliance, contact:
- **Email**: admin@hontru.com

## Schedule A: Details of Processing
### A.1 Subject Matter and Duration
- **Subject Matter**: Processing Personal Data to provide the Services, including AI-driven tutoring, collaborative learning platforms, and user account management.
- **Duration**: For the term of the Agreement, or until Personal Data is returned or deleted per Section 9.

### A.2 Nature and Purpose
- **Nature**: Collection, storage, organization, use, disclosure, and deletion of Personal Data to deliver and improve the Services.
- **Purpose**: To enable educational and professional functionalities, such as personalized learning, mentorship, and collaboration, and to comply with legal obligations.

### A.3 Types of Personal Data
- Identifiers (e.g., names, email addresses, student IDs).
- Educational data (e.g., academic records, performance metrics).
- Communication data (e.g., messages within the platform).
- Usage data (e.g., interactions with AI tutors, session logs).
- Sensitive Data, if provided (e.g., health or ethnic data, subject to strict safeguards).

### A.4 Categories of Data Subjects
- Students enrolled in Educational Institutions using the Services.
- Educators and administrators affiliated with Educational Institutions.
- Other users (e.g., professionals, mentors) accessing the Services.

### A.5 Obligations and Rights
- HonTru LLC’s obligations are as outlined in this DPA (e.g., security, Sub-processor management).
- Your rights include providing Instructions, auditing compliance, and objecting to Sub-processors.

# Trademark Policy

This Trademark Policy governs the use of trademarks owned by HonTru LLC, including those associated with our web and mobile applications, such as Mentor AI and School AI (collectively, the "Services"). HonTru LLC's trademarks are valuable corporate assets that represent our brand's reputation for innovative educational technology and mentorship solutions. This policy outlines permissible and prohibited uses to protect our trademarks and ensure clarity for users, including Educational Institutions, Educators, Students, and other third parties.

**1. Scope of Trademarks**

HonTru LLC reserves all rights to its trademarks, which include:

- The "HonTru" name and logo.
- Product and service names, such as "Mentor AI," "School AI," and "HonTru AIStudent."
- Other logos, designs, slogans, or branding elements owned by HonTru LLC, whether registered or unregistered.

These trademarks (collectively, "HonTru Trademarks") are protected under U.S. and international trademark laws. Unauthorized use may result in legal action to prevent infringement or dilution.

**2. Permissible Use of Logos**

Use of HonTru LLC logos (e.g., the HonTru corporate logo or product-specific logos) is strictly limited. You may only use HonTru LLC logos if:

- You have express written permission from HonTru LLC, obtained by contacting admin@hontru.com.
- You are a licensed partner or authorized user under a written agreement with HonTru LLC.

Permitted use must comply with:

- This Trademark Policy.
- Any license terms or usage guidelines provided by HonTru LLC.
- HonTru LLC's Brand Guidelines, available upon request.

Logos must be used in their original form, without alteration, and in a manner that does not imply endorsement or affiliation beyond the authorized relationship.

**3. Fair Use of Trademarks**

"Fair use" of HonTru Trademarks, without express permission or license, is limited to text-only references to HonTru LLC's product or service names (e.g., "Mentor AI" or "School AI"). Fair use excludes logos and graphical elements. To qualify as fair use, you must:

- Be truthful and accurate in your references.
- Avoid disparaging HonTru LLC, its Services, or its reputation.
- Clearly indicate that your products, services, or organization are not affiliated with or endorsed by HonTru LLC, unless explicitly authorized.
- Use HonTru Trademarks only to describe HonTru LLC's Services (e.g., "Our school uses Mentor AI for tutoring") and not as part of your own branding.

**3.1 Attribution and Marking**

When using HonTru Trademarks in text:

- The first reference to each trademark must include the appropriate symbol:
  - Registered trademarks: ® (e.g., HonTru®).
  - Unregistered trademarks: ™ (e.g., Mentor AI™).
- Include a footnote or statement acknowledging HonTru LLC's ownership, such as: "HonTru, Mentor AI, and School AI are trademarks of HonTru LLC."
- Use the exact spelling and capitalization (e.g., "HonTru," not "Hontru" or "HONTRU").

**4. Prohibited Uses**

To protect the integrity of HonTru Trademarks and prevent confusion, dilution, or harm to HonTru LLC's reputation, the following uses are strictly prohibited without prior written consent:

- Using HonTru LLC logos or graphical elements in any form, including on websites, marketing materials, or products.
- Altering, adapting, or modifying any HonTru Trademark (e.g., changing colors, fonts, or proportions).
- Using a HonTru Trademark in a way that suggests your products, services, or organization are affiliated with, endorsed by, or originate from HonTru LLC, unless authorized.
- Incorporating a HonTru Trademark into your company, product, service, or program name (e.g., “HonTru Tutoring”).
- Using a HonTru Trademark in a manner that dilutes, defames, disparages, or harms HonTru LLC’s reputation, such as associating it with counterfeit or unauthorized products.
- Registering or attempting to register any trademark, name, or designation confusingly similar to a HonTru Trademark.
- Registering or using a domain name that incorporates a HonTru Trademark (e.g., “hontruapp.com”).
- Copying or imitating HonTru LLC’s website design, type style, product packaging, or overall brand aesthetic.
- Using a HonTru Trademark as a noun or in plural form (e.g., say “Mentor AI platform” instead of “Mentor AIs”).
- Combining HonTru Trademarks with unauthorized or counterfeit products, software, or services.

**5. Enforcement**

HonTru LLC actively monitors and enforces its trademark rights to prevent infringement, dilution, or misuse. If we identify unauthorized use, we may:

- Request immediate cessation of the use.
- Pursue legal remedies, including injunctions, damages, or attorney’s fees, under U.S. and international trademark laws.
- Terminate any licenses or permissions associated with the Services, per the Terms of Service.

To report suspected trademark misuse, contact admin@hontru.com.

**6. Guidelines for Authorized Users**

If you are an authorized user (e.g., a licensed Educational Institution or partner), you must:

- Adhere to HonTru LLC’s Brand Guidelines, provided upon licensing.
- Use HonTru Trademarks only within the scope of your agreement (e.g., for promoting Mentor AI within your institution).
- Submit proposed uses for review if required by your license.
- Promptly correct any non-compliant use upon HonTru LLC’s request.

**7. Disclaimer**

This Trademark Policy is not legal advice. For questions about your legal rights or obligations regarding trademark use, consult your own attorney. HonTru LLC is not responsible for any third-party misuse of its trademarks or for your compliance with this policy.

**8. Contact Information**

For questions, permission requests, or to report trademark concerns, contact:

- **Email**: admin@hontru.com

# Security and Reliability Safeguards

At HonTru LLC, we recognize that our customers, including Educational Institutions, Educators, Students, and professionals, rely on our Services—such as Mentor AI and School AI—as critical components of their educational and business processes. We prioritize the security, reliability, and privacy of our software, systems, and data to ensure trust and compliance with applicable laws, including the General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), and Payment Card Industry Data Security Standard (PCI DSS). This Security and Privacy Statement outlines the measures we take to protect your data and maintain the integrity of our Services.

**1. Data Encryption**

We use industry-standard encryption to safeguard data transmitted between your device and our Services:

- **In Transit**: All communications are protected with 256-bit Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption. The lock icon in your browser verifies that you're connecting to HonTru LLC's legitimate servers, not a phishing site.
- **At Rest**: Sensitive data, including Student Data and cardholder information, is encrypted using AES-256, ensuring protection against unauthorized access.

**2. Firewalls and Network Security**

Our Services, including all customer data, are hosted behind robust firewalls to prevent unauthorized access. These firewalls are:

- Configured to filter and monitor incoming and outgoing traffic.
- Regularly updated to address emerging threats, ensuring a secure environment for your data.

**3. Vulnerability Management**

To maintain system integrity, we conduct:

- **Regular Vulnerability Scanning**: Our servers are scanned weekly for vulnerabilities using industry-standard tools, with immediate remediation of identified issues.
- **Penetration Testing**: Annual third-party penetration tests assess our defenses, ensuring proactive protection against exploits.

**4. Physical Security**

Our servers are hosted in state-of-the-art data centers with:

- **Biometric Access Controls**: Restricting entry to authorized personnel only.
- **24/7 Surveillance**: Continuous monitoring to prevent unauthorized access.
- **Environmental Protections**: Redundant power feeds, backup generators, advanced fire suppression, and climate control to ensure server reliability.
- **Geographic Redundancy**: Data centers in multiple locations to mitigate risks from natural disasters or disruptions.

**5. PCI Compliance and Cardholder Data**

For customers using payment features (e.g., recurring templates), we handle cardholder data in compliance with PCI DSS Level 1 requirements:

- **Secure Input**: Cardholder data may only be entered in designated fields explicitly designed for payment processing.
- **Trusted Partners**: We leverage PCI DSS Level 1-compliant payment processors (e.g., Stripe) for secure storage and processing, audited annually by independent third parties.
- **Annual Audits**: HonTru LLC maintains its own PCI DSS Level 1 compliance through annual audits by a Qualified Security Assessor (QSA), ensuring adherence to strict security standards.

**6. Secure Development Practices**

Our development team adheres to secure coding standards to minimize vulnerabilities:

- **OWASP Guidelines**: We follow the Open Web Application Security Project (OWASP) Top Ten best practices to address risks like injection attacks and cross-site scripting.
- **Principle of Least Privilege**: Developers and systems access only the data and resources necessary for their functions, reducing exposure risks.
- **Code Reviews and Testing**: All code undergoes peer reviews and automated security

testing before deployment.

**7. Data Breach Notification**

In the event of a security or privacy breach (e.g., unauthorized access, loss, or disclosure of data), we will:

- Notify affected customers and relevant authorities (e.g., Supervisory Authorities under GDPR, or institutions under FERPA) within legally required timelines, typically within 72 hours of discovery, per GDPR Article 33 and web:2.
- Provide details of the breach's scope, impact, and mitigation steps, as outlined in our Data Breach Response Checklist (aligned with web:0).
- Cooperate with customers to address and remediate the incident.

**8. Reliability and Redundancy**

To ensure uninterrupted access to our Services, we maintain:

- **Redundant Infrastructure**: Servers and storage are replicated across multiple nodes to prevent data loss or downtime from hardware failures.
- **Geographic Distribution**: Data is mirrored in geographically separate data centers, ensuring availability in case of a primary data center outage (e.g., due to natural disasters).
- **Uptime Monitoring**: Continuous monitoring and automated failover systems to maintain service availability.

**9. Managed Hosting**

We host our Services on Microsoft Azure, a leading cloud platform known for:

- **Scalability**: Supporting rapid feature delivery and innovation to meet customer needs.
- **Security**: Providing robust security controls, including encryption, access management, and compliance certifications (e.g., ISO 27001, SOC 2).
- **Reliability**: Minimizing downtime through redundant infrastructure and global availability zones.

**10. Data Backups**

To protect against data loss, we implement:

- **Real-Time Replication**: Data is replicated across multiple database servers in two geographic regions, ensuring no single failure results in data loss.
- **Regular Backups**: Automated daily backups are encrypted and stored securely, with retention periods compliant with GDPR and FERPA requirements.
- **Restoration Capabilities**: Rapid recovery processes to restore data in case of accidental deletion or system failure, minimizing disruption.

**11. Compliance with Data Protection Laws**

Our security practices align with applicable data protection laws, including:

- **GDPR**: For EU users, we adhere to the Data Processing Addendum (artifact_id: 6fc3cca3-ae6f-4522-a1d7-c2d5b2ba7901), ensuring secure processing of Personal Data.
- **FERPA**: For U.S. educational users, we protect Student Data per the Student Data Privacy Addendum in our Terms of Service (artifact_id: bab8b11c-313a-48a1-9257-885afc8abc3f).
- **COPPA**: We rely on Educational Institutions for parental consent for users under 13, per web:2.
- **State Laws**: Compliance with laws like California's SOPIPA, ensuring Student Data protection.

**12. Customer Responsibilities**

To maximize security, we encourage customers to:

- Use strong, unique passwords and enable multi-factor authentication (MFA) where available.
- Enter sensitive data (e.g., cardholder information) only in designated fields.
- Promptly report suspected security issues to admin@hontru.com.
- For Educational Institutions, ensure compliance with FERPA and COPPA consent requirements.

**13. Contact Information**

For questions about our security practices or to report concerns, contact:

- **Email**: admin@hontru.com

# Cookie Policy

HonTru LLC, its affiliates, and brands (“we,” “us,” or “HonTru LLC”) use cookies and similar tracking technologies on our websites (e.g., https://www.hontru.com/) and Services, including Mentor AI and School AI, to enhance your experience, deliver personalized content, and improve our platforms.

**1. What Are Cookies and Similar Technologies?**

Cookies are small text files placed on your computer or mobile device by a web server when you visit our websites or use our Services. They store information to improve your browsing experience, such as remembering your login status or preferences. Similar technologies include web beacons, pixels, and local storage, which serve comparable functions. These technologies help us understand user behavior, customize content, and ensure the functionality of our Services.

**2. Why We Use Cookies**

We use cookies and similar technologies for the following purposes:

- **Essential Operations**: To enable core functionalities of our Services, such as user authentication and session management.
- **Performance and Analytics**: To monitor usage, measure performance, and improve our Services.
- **Personalization**: To tailor content and features to your preferences, enhancing your experience.
- **Marketing and Advertising**: To deliver relevant promotions and ads, including through third-party platforms.
- **Social Media and Content**: To integrate social media features and enhance interactive content.

For users in educational contexts (e.g., Students, Educators), we ensure that cookies respect privacy obligations under laws like GDPR, COPPA, and FERPA, as outlined in our Terms of Service.

**3. Types of Cookies We Use**

We categorize cookies based on their purpose and function. Below are the types we use, along with examples and their roles:

**3.1 Strictly Necessary Cookies**

These cookies are essential for the operation of our Services and cannot be disabled. They enable features like:

- User authentication (e.g., maintaining your login status during a session).
- Security measures (e.g., detecting fraudulent activity).
- Navigation and core functionality (e.g., accessing Mentor AI tutoring features). **Example**: Session cookies that track your identity for the duration of your visit.

**3.2 Functional Cookies**

These cookies enhance your experience by remembering your preferences and customizing content. They may be set by us or third-party providers, such as:

- Hello Bar: Displays personalized messages or notifications.
- Proof: Customizes website interactions based on user behavior. **Example**: A cookie that remembers your language preference on our website.

**3.3 Analytics and Performance Cookies**

These cookies collect anonymized data to analyze how users interact with our Services, helping us improve functionality and user experience. We use tools like:

- Google Analytics: Tracks page views, session duration, and feature usage.

- Other third-party analytics providers: Provide insights into user behavior. **Example**: A cookie that records how often you visit our tutoring platform to optimize content delivery.

For more on Google Analytics, visit Google's Privacy Information.

**3.4 Marketing and Advertising Cookies**

These cookies support our marketing efforts by delivering personalized ads and tracking campaign effectiveness. They may be set by us or third-party advertisers and typically do not collect personally identifiable information. They include:

- Ad platforms: Tailor ads based on your interests across websites.
- Tracking pixels: Measure ad performance and user engagement. **Example**: A cookie that notes you visited our marketing page to show relevant ads on third-party sites.

**3.5 Social Media and Content Cookies**

These cookies enable social media integration and interactive content, set by third-party services like:

- Facebook, Twitter, or LinkedIn plugins: Allow sharing or liking content.
- Video platforms (e.g., YouTube, Vimeo): Embed tutorials or demos.
- Commenting systems: Facilitate user discussions. **Example**: A cookie set by a Facebook "Like" button to track engagement with our blog posts.

These cookies may also support behavioral advertising or analytics by third parties, subject to their privacy policies.

**4. Cookies and Student Data**

For users under 18, particularly Students using Student-Facing Services (e.g., HonTru School AI), we take additional precautions:

- We do not use marketing or advertising cookies for Student accounts, per COPPA and FERPA requirements (web:2).
- Analytics cookies are anonymized and used only to improve educational features, with data processing authorized by Educational Institutions, per our Student Data Privacy Addendum (artifact_id: bab8b11c-313a-48a1-9257-885afc8abc3f, Section 12.3).
- Parental or institutional consent is obtained for users under 13, as required by COPPA, and for users under 16 in the EU, per GDPR Article 8.

**5. How We Manage Cookies**

- **First-Party Cookies**: Set directly by HonTru LLC to manage core functions and personalization.
- **Third-Party Cookies**: Set by trusted partners (e.g., Google, Facebook) for analytics, advertising, or social features, subject to their privacy policies and our Data Processing Addendum (artifact_id: 6fc3cca3-ae6f-4522-a1d7-c2d5b2ba7901).
- **Retention**: Cookies are retained only as long as necessary for their purpose (e.g., session cookies expire when you close your browser; persistent cookies may last up to 12 months unless deleted).
- **Security**: Cookies containing personal data are encrypted and stored securely, per our Security and Privacy Statement (artifact_id: 6be053a5-ab31-438f-b1de-221b7a5a9c88).

**6. Your Cookie Choices**

You can manage cookies through the following options:

- **Browser Settings**: Most browsers allow you to block, delete, or manage cookies. For guidance, consult your browser's help documentation:
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
- **Opt-Out Tools**:

  - **Google Analytics**: Install the Google Analytics Opt-out Browser Add-on or adjust settings on your Google Ads Settings.
  - **Advertising Networks**: Use the Network Advertising Initiative (NAI) Opt-Out Tool to disable interest-based ads from participating providers.
- **Device Settings**: On mobile devices (e.g., iPhone, Android), adjust privacy settings to limit ad tracking:
  - iOS: Go to Settings > Privacy > Advertising > Limit Ad Tracking.
  - Android: Go to Settings > Google > Ads > Opt out of Ads Personalization.
- **Cookie Consent Banner**: On our websites, you can manage non-essential cookies via our consent banner (for EU users, per GDPR and e-Privacy Directive).

**Note**: Blocking or deleting cookies may impact your experience, as some features (e.g., auto-login, personalized tutoring) may not function fully. Strictly Necessary Cookies cannot be disabled, as they are essential for Service operation.

**7. Compliance with Applicable Laws**

Our cookie practices comply with:

- **GDPR and e-Privacy Directive**: For EU users, we obtain consent for non-essential cookies and provide clear opt-out options, per GDPR Article 7 and e-Privacy Directive (web:0).
- **COPPA**: We limit cookie use for users under 13, relying on Educational Institutions for consent, per web:2.
- **FERPA**: Student Data collected via cookies is protected under our Student Data Privacy Addendum, ensuring educational use only.
- **State Laws**: Compliance with laws like California's Consumer Privacy Act (CCPA), where applicable, for transparency and control.

**8. Updates to This Notice**

We may update this Cookie Notice to reflect changes in our practices, technologies, or legal requirements. Updates will be posted on https://www.hontru.com/, and significant changes will be communicated via email or our Services interface. Continued use of our Services after updates constitutes acceptance of the revised notice.

**9. Contact Information**

For questions about our cookie practices or to exercise your privacy rights, contact:

- **Email**: admin@hontru.com

# Google Data Use Disclosure

HonTru LLC - use and transfer to any other app of information received from Google Accounts will adhere to Google API Services User Data Policy, including the Limited Use requirements.

# Treatment of Google User Data

Notwithstanding anything to the contrary herein, if you provide the Service access to certain types of your Google data, the Service's use of that data will be subject to these additional restrictions:

The Service will only use access to read, write, modify or control Google Drive, Tasks, Google Calendar and Gmail message bodies (including attachments), documents, events, metadata, headers, and settings to provide a web email client that allows users to compose, send, read, and process emails and will not transfer this Gmail data to others unless doing so is necessary to provide and improve these features, comply with applicable law, or as part of a merger, acquisition, or sale of assets.

The Service will not use this Gmail, Google Drive, Tasks and Google Calendar data for serving advertisements. The Service will not allow humans to read this data unless we have your affirmative agreement for specific messages, doing so is necessary for security purposes such as investigating abuse, to comply with applicable law, or for the Service's internal operations and even then only when the data have been aggregated and anonymized.

# Email Integration Privacy Disclosure

Users of HonTru LLC, may utilize the email integration feature to import email messages from third-party providers such as Google's Gmail API, Drive API, Calendar API, Tasks API and Microsoft's Outlook API. HonTru LLC, adheres to the following data processing, handling and storage policies:

Integration data including but not limited to email messages, attachments and accompanying metadata will not be shared with any entity or service provider that is not part of HonTru LLC Data will be accessible only to users authorized by the original account owner.

Data can be permanently removed from HonTru LLC, databases and other storage means upon user request. Such requests are handled automatically by our system and are immediately executed. Data will not be used for serving ads, including retargeting, personalized, or interest-based advertising. Data will not be accessed by humans, unless an affirmative agreement has been obtained from the user to view specific messages, files, or other data, with the limited exception of use cases approved by Google under additional terms applicable to the Nest Device Access program;

It is necessary for security purposes (such as investigating a bug or abuse); It is necessary to comply with applicable law; or Its use is limited to internal operations and the data (including derivations) have been aggregated and anonymized.