ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

1050 Main Street
Roseville, CA 95678
Phone (916) 771-1645

Data Privacy Agreement

This Agreement is entered into between the **Roseville City School District** ("LEA" or "District") and

Everway LLC
"Service Provider" or "Vendor"

("Service Provider" or "Vendor") on

09/02/2026
Effective Date

WHEREAS, the LEA and the Service Provider entered into an agreement for educational or digital services to the LEA;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed, or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms; and

WHEREAS, the provider and LEA agree that additional and modified sections are required to address the use of Artificial Intelligence ("AI") as part of the services or product provided;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. PASSWORD SECURITY: All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator, or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Vendor Attestation:

Agree

2. SYSTEM SECURITY: Unauthorized access to or modification of District systems, including file servers, routers, switches, NDS, and Internet services, is prohibited. Any attempt to bypass or subvert any District security system, both hardware and software, is prohibited.

Vendor Attestation:

Agree

3. PRIVACY: The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code, and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties protected and confidential. Release of this data can be authorized only by Technology Services management and by state and federal law.

Vendor Attestation:

Agree

4. REUSE: Vendors shall not copy, duplicate, sell, repackage, or use for demonstration purposes any Roseville City School District data without the prior written consent of Educational or Technology Services management.

Vendor Attestation:

Agree

5. TRANSPORT: The Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

Vendor Attestation:

Agree

6. EXTERNAL SECURITY: The Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Vendor Attestation:

Agree

7. INTERNAL SECURITY: Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personnel (or their representatives) will have directly with District data. How is the data uploaded from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protect against unauthorized access to District data? How are backups performed, and who has access to and custody of the backup media? How long are backups maintained? What happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard-copy records?

Vendor Attestation:

Agree

8. DISTRICT ACCESS: The Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Vendor Attestation:

Agree

9. TERMINATION: Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. The Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Vendor Attestation:

Agree

Section II: AB1584 Compliance - Student Information Only

1. The Vendor agrees that the Roseville City School District retains ownership and control of all student data.

Vendor Attestation:

Agree

2. The Vendor must attach a description of how student-created content can be exported and/or transferred to a personal account to this document.

Vendor Attestation:

Not Applicable

Export Student-Created Content Not Applicable

Content stays within the product.

3. The Vendor is prohibited from allowing third parties access to student information beyond those purposes defined in the contract.

Vendor Attestation:

Agree

4. The Vendor must attach a description of how parents, legal guardians, and students can review and correct their personally identifiable information to this document.

Vendor Attestation:

Agree

5. The Vendor will attach to this document evidence of how student data is kept secure and confidential.

Vendor Attestation:

Agree

6. The Vendor will attach to this document a description of the procedures for notifying affected parents, legal guardians, or eligible students when student records are unauthorizedly disclosed.

Vendor Attestation:

Agree

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled.

Vendor Attestation:

Agree

8. The Vendor will attach to this document a description of how they and any third-party affiliates comply with FERPA.

Vendor Attestation:

Agree

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students.

Vendor Attestation:

Agree

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Vendor Attestation:

Agree

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Vendor Attestation:

Agree

3. Vendors cannot sell student information.

Vendor Attestation:

Agree

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety, or operational improvement reasons.

Vendor Attestation:

Agree

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Vendor Attestation:

Agree

6. Vendors must delete district-controlled student information when requested by the District.

Vendor Attestation:

Agree

7. Vendors must disclose student information when required by law, for legitimate research purposes, and for school purposes to educational agencies.

Vendor Attestation:

Agree

Section IV: Audit and Compliance Oversight

1. Audit Rights. The District reserves the right to audit the Vendor's privacy and security practices no more than once annually or at any time in response to a data incident, suspected noncompliance, or legal/regulatory inquiry. The Vendor shall provide reasonable access to systems, records, and personnel involved in the handling of District data.

2. Confidentiality Agreement. RCSD agrees to execute a reasonable non-disclosure agreement to protect Vendor trade secrets or proprietary information disclosed during the audit.

3. Framework Compliance. Vendor agrees to implement and maintain security controls consistent with one or more of the following frameworks:

a. NIST Cybersecurity Framework (NIST CSF)

b. NIST SP 800-53 or 800-171

c. ISO/IEC 27001

d. CIS Critical Security Controls (Top 18)

The Vendor shall indicate which framework is used and provide a summary upon request.

Designated Security Framework(s):

Everway LLC maintains an ISO 27001:2022 certification

4. Security Program Documentation. Upon request, the Vendor shall furnish RCSD with the following:

a. A summary of its data security policies and incident response procedures.

b. Results from the most recent third-party security assessment or audit, redacted as necessary.

c. Any certifications (e.g., SOC 2, ISO 27001).

5. Remediation Obligations. If a security deficiency or compliance failure is identified, the Vendor shall deliver a written remediation plan to RCSD within thirty (30) days. The District may suspend access to its data until the deficiency is addressed to the District's satisfaction.

6. Subprocessor Oversight. The Vendor is responsible for ensuring that all subprocessors or affiliates with access to District data comply with the terms of this agreement and are subject to equivalent audit and compliance obligations.

Exhibits

Section 1.6: External Security

Everway protects its cloud infrastructure and web applications from external attacks using layered security controls, including managed firewalls, network segmentation, NAT, IDS/IPS and continuous threat monitoring. Vulnerability scanning and regular penetration testing are performed to identify and remediate security weaknesses. These controls are managed under Everway's ISO/IEC 27001:2022 certified Information Security Management System.

Section 1.7: Internal Security

We manage technical security solutions to ensure the security and resilience of our systems and assets. We implement firewalls, IDS/IPS, network segmentation, endpoint protection, encryption, and strict access controls. We apply security patches regularly, monitor for threats 24/7, and conduct vulnerability scans and penetration tests. Our cloud and physical infrastructure are protected by ISO 27001-certified controls, and we enforce policies and procedures for risk mitigation, access management, and incident response. Regular audits and continuous improvement ensure alignment with policies, procedures, and agreements

Section II.2: Exporting of Student-Created Content

N/A

Section II.4: Review and Correct Personally Identifiable Information (PII)

In most cases it can be corrected by contacting the district employee that created/maintained the data. If further help is needed, you have the right to request access to or correction of your personal information at any time. You can make such a request by contacting Everway using an online form. Everway customer support is available at na-support@everway.com

Section II.5: Securing Student Data

We implement robust data security standards, including encryption of data in transit (TLS 1.2+) and at rest (AES-256), strict access controls with two-factor authentication, and regular internal and external audits. We review security policies annually, securely wipe data before equipment disposal, and require regular security training for all employees. Our cloud providers comply with ISO 27001

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Everway employs commercially reasonable security measures that comply, in Everway's reasonable discretion and interpretation, with all applicable Federal and state laws and regulations regarding data privacy and security, including but not limited to the Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act of 1998 ("COPPA"). These measures include appropriate administrative, physical, and technical safeguards to secure data from unauthorized access, disclosure, alteration, and use. Everway will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Except as expressly provided in this Agreement, neither Everway nor its successors or assigns shall have any liability for the breach of its privacy and security measures or the integrity of its hosting services, unless caused by the willful misconduct of Everway. Everway expressly disclaims any warranty that data exchanges are or will be secure. All Everway employees and third-party contractors receive annual training concerning student data privacy.

Section III.5: How Student Data is Protected:

Data is stored in US based Microsoft Azure and AWS data centers with cloud providers that are audited and certified for secure handling of data. We protect data through strong encryption (TLS 1.2, AES-256), strict access controls, and multi-factor authentication. Regular audits, employee training, and an incident response plan ensure ongoing security. We minimize data collection, enforce secure retention and disposal, and assess third-party vendors to maintain high protection standards

Required Security & Compliance Attachments

Please upload all required documentation referenced in this agreement, including evidence of external and internal security controls, data protection practices, compliance certifications (e.g., SOC 2, ISO 27001), incident response procedures, and any required FERPA, SOPIPA, or AB 1584 compliance documentation.

Attachments should clearly correspond to the sections outlined in the Data Privacy Agreement.

Upload

[Private File Not Included]

[Private File Not Included]

[Private File Not Included]

ARTIFICIAL INTELLIGENCE (AI) ADDENDUM

Section A: Applicability Declaration

Please select the appropriate response below:

◉ Option 1: Applicable (AI Deployment Active) ○ Option 2: Not Applicable (No AI Deployment)

Option 1: Applicable (AI Deployment Active)

The Service Provider currently uses, embeds, or leverages AI features, models, or third-party AI sub-processors to deliver Services to the District.

- **Required:** Provider must comply with all sections of this Addendum.
- **Action:** Review all requirements and execute the signature block below.

Option 2: Not Applicable (No AI Deployment)

The Service Provider does not currently use, embed, or leverage AI features or third-party AI services in connection with District Student Data or Services.

- **Waived:** Sections 1 and 3–10 do not apply.
- **Required:** Provider must comply with Section 2.1 (Future Deployment Notification).
- **Action:** Sign the signature block below to execute this waiver.

Section B: AI Governance Terms

1. AI Usage Limitations, Ownership & Third-Party Models

1.1. The Service Provider shall not use, transfer, or reproduce Student Data for Artificial Intelligence (AI) training, model development, fine-tuning, or content generation without the District's prior written consent. The Provider agrees to uphold the principles outlined in California Education Code §33328.5, ensuring that any AI systems used in connection with the Service align with values of equity, safety, transparency, and accountability in the interest of student welfare.

1.2. Sub-licensing Student Data for such purposes is strictly prohibited unless explicit written permission is obtained from the student's parent, legal guardian, or eligible student.

1.3. Ownership of all Student Data, including content generated with AI assistance, remains with the District or the student, as applicable.

2. Notification and Consent

2.1. If any feature of the Service is modified to include AI functionality (or if a non-AI provider intends to introduce AI features), the Provider shall notify the District in writing prior to deployment.

2.2. The Provider must disclose the specific AI architecture (including third-party tools used), the purpose of such use, and how Student Data will be processed within these features.

2.3. No AI feature may be enabled until the District provides written consent and has reviewed any updated data-handling practices.

3. Algorithm Bias and Fairness

3.1. The Provider certifies that any AI technologies used in facilitating the Services (whether proprietary or integrated via third parties) are regularly audited for algorithmic bias and fairness.

3.2. Upon request by the District, the Provider shall furnish a summary of audit findings related to bias detection and mitigation strategies. For third-party embedded AI, providing official third-party audit reports or compliance attestations shall satisfy this requirement. These audits shall demonstrate commitment to promoting equitable outcomes and addressing systemic bias under California Education Code §33328.5(d).

4. AI Hallucinations and Reliability

4.1. The Provider shall monitor the hallucination rate of any deployed generative AI models (e.g., large language models or chatbots) and employ industry-standard techniques to reduce the occurrence of inaccurate or misleading outputs.

4.2. The Provider shall maintain a mechanism for the District to report hallucinated or harmful responses and address such issues in a timely and accountable manner

5. Prohibited Uses of AI

The Provider shall not (and shall ensure its sub-processors do not):

5.1. Use AI to generate synthetic or inferred Student Data.

5.2. Develop behavioral profiles for marketing or advertising.

5.3. Engage in predictive analytics that may result in automated decision-making affecting students without human oversight.

5.4. Deploy AI systems that are not designed to minimize harmful outcomes to minors, including but not limited to biased academic profiling or discriminatory content outputs.

These prohibitions align with California Education Code §33328.5(c), which calls for educational AI technologies to be designed to minimize harm and safeguard the well-being of students.

6. Student Content and AI-Generated Work

If students create content using AI tools embedded in the Service (e.g., essays, responses, or projects), the Provider shall:

6.1. Ensure students can download or export that content.

6.2. Retain no ownership or claim over AI-assisted student work.

6.3. Maintain logs of AI interactions in accordance with FERPA.

6.4. Support digital literacy and public awareness regarding the use of AI, in accordance with §33328.5(b), by enabling users to understand when they are interacting with an AI system.

7. Transparency and Disclosure Requirements (SB 942)

7.1. To the extent required by California SB 942, the Provider shall maintain and make available tools or mechanisms to verify whether content was generated by AI, including provenance data where applicable. This tool shall:

7.1.1. Provide provenance data (excluding personal data).

7.1.2. Support multiple content formats.

7.1.3. Accept user feedback to support continuous improvement.

7.2. All AI-generated content must include latent disclosures that identify:

7.2.1. The Provider's name.

7.2.2. Identification of the AI system used.

7.2.3. The creation date and time.

7.2.4. A unique identifier for the generated content.

7.3. The Provider shall also offer users the option to include visible disclosures indicating that the content was generated by AI. These disclosures must be conspicuous and designed to resist removal.

7.4. If the Provider licenses its AI technology to third parties, such license agreements shall require those third parties to uphold the same transparency and disclosure standards outlined herein.

8. Third-Party AI Sub-processors & Embedded Tools

8.1. Flow-Down Obligations: If the Provider embeds, integrates, or queries third-party AI models or APIs (e.g., OpenAI, Anthropic, Azure OpenAI), the Provider remains fully responsible for ensuring such third parties comply with the privacy, non-training, and security standards set forth in this Addendum.

8.2. Zero-Data Retention / No Training Guarantee: The Provider certifies that all third-party AI integrations operate under enterprise API agreements that strictly prohibit the third-party AI vendor from retaining, logging, or using Student Data to train their underlying models.

8.3. Exemptions for Standard Third-Party Infrastructure: Where the Provider leverages external foundation models, compliance with Sections 3 (Auditing) and 7 (Provenance) may be fulfilled by providing the underlying vendor's published safety, transparency, and audit documentation.

9. Definitions

9.1. Artificial Intelligence (AI): Systems that analyze data and take actions, with some degree of autonomy, to achieve specific goals.

9.2. Hallucination: A response generated by an AI system that is incorrect, nonsensical, or misleading while appearing factually accurate.

9.3. Algorithmic Bias: Systematic and unfair discrimination in outcomes generated by an algorithm based on characteristics such as race, gender, or disability.

10. Compliance with State Advisory Guidelines

10.1. The Provider shall monitor and cooperate with any guidance or recommendations issued by the California Department of Education's Artificial Intelligence in Education Advisory Council, as established under Education Code §33328.5(a). This cooperation may include participation in feedback initiatives, alignment with recommended practices, or revisions to data governance protocols in response to evolving regulatory requirements.

Service Provider Signature

Claire McKreavey

Date Signed

09/02/2026 04:56 pm

DATA INCIDENT NOTIFICATION ADDENDUM

This Exhibit outlines the Vendor's obligations in the event of a Data Incident involving Customer Data. These obligations are in addition to and do not limit any rights or remedies available to the Customer under the Agreement or applicable law.

1. Data Incident Notification

1.1. In the event Roseville City School District ("RCSD" or "District" or "Customer") Data is accessed, acquired, or reasonably believed to have been accessed or acquired by an unauthorized individual or third party ("Data Incident"), the Vendor shall notify the Customer in writing without undue delay, and in no case later than seventy-two (72) hours after confirming the occurrence of the Data Incident.

1.2. The Vendor shall comply with all reasonable instructions from the District in relation to the Data Incident and, in consultation with the District, take all appropriate and reasonable steps to investigate and mitigate any known or anticipated harmful effects resulting from such unauthorized access, use, or disclosure of Customer Data.

1.3. If the Data Incident involves Personally Identifiable Data (PII), including but not limited to Social Security numbers, government-issued identification numbers, financial account details, health records, or medical information protected under applicable privacy laws (e.g., HIPAA, FERPA, CCPA, SOPIPA, GDPR, CRPA, etc), the Vendor shall apply heightened protections in accordance with applicable state and federal law, including but not limited to breach notification, identity theft prevention, and mitigation requirements.

2. Notification to Affected Individuals and Authorities

The obligations in this Section apply in all cases where the Data Incident is caused, in whole or in part, by the actions or omissions of the Vendor, its subcontractors, or affiliates.

2.1. Following confirmation of a Data Incident, the vendor shall provide written notification to affected individuals whose data was compromised. This notification shall:

2.1.1. Be written in plain language;

2.1.2. Be delivered in compliance with applicable federal, state, or provincial laws;

2.1.3. Be issued without unreasonable delay following the District's approval and any required consultation with law enforcement

2.2. The notification to affected individuals shall include, at a minimum:

2.2.1. A general description of the incident and the Vendor's response efforts.

2.2.2. The contact information of the Vendor's designated incident response representative.

2.2.3. The type(s) of Customer Data or PII involved (e.g., name, address, date of birth, Social Security number, student records, health/medical information, etc.);

2.2.4. The known or estimated date(s) of the Data Incident and the date of notification.

2.2.5. Whether law enforcement was involved and whether any delay in notification was due to a law enforcement investigation.

2.2.6. Steps the individual can take to protect themselves.

2.3. The Vendor agrees to adhere to all applicable federal, state, and provincial laws concerning the protection of Customer Data, including but not limited to the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act (HIPAA), where applicable.

In the event of a Data Incident involving Personally Identifiable Information (PII) of a minor, the Vendor acknowledges that PII includes both direct and indirect identifiers that could reasonably identify an individual student. Under FERPA, PII includes, but is not limited to:

- Student's full name
- Student identification number or state/local student identifier
- Date and/or place of birth
- Grade level or classroom assignment
- School name or teacher name
- Mailing address or contact information
- Parent/guardian names and contact information
- Any combination of the above elements that would reasonably allow identification of the student with reasonable certainty

2.4. If such PII is involved in a Data Incident, the Vendor shall:

2.4.1. The Vendor shall fully fund and coordinate identity monitoring and/or credit monitoring services for a minimum of twelve (12) months, including, at a minimum, dark web monitoring, identity theft insurance, and access to fraud resolution agents, without cost to the affected individual or the District.

2.4.2. As described in Section 2.2, notify all affected individuals (or their legal guardians, as applicable).

2.4.3. If five hundred (500) or more individuals are affected, the Vendor shall notify the appropriate State Attorney General or supervisory authority in accordance with relevant state data breach laws and ensure that the notification complies with all timing, format, and content requirements set forth under the relevant state's breach notification statute. A copy of the regulatory notification shall be provided to the Customer.

2.4.4. Maintain a record of the Data Incident, including the nature of the breach, categories of data affected, notification steps taken, and services provided. Upon request, the customer will have access to these records.

2.4.5. The Vendor shall ensure that all breach response and notification processes are consistent with applicable FERPA guidance and any other relevant federal, state, or provincial privacy regulations. No PII shall be re-disclosed or shared with any third party, including subcontractors or affiliated entities, without prior written consent from the District or as explicitly required by law. The Vendor shall document and maintain detailed records of all data disclosures related to the incident and shall make those records available to the District upon request.

3. Legal Compliance and Risk Management

The Vendor agrees to comply with all applicable local, state, provincial, and federal data privacy and security laws, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA)

State-specific data breach notification statutes

3.1. The Vendor shall maintain a written incident response and breach notification policy that complies with industry standards and applicable law. The Vendor shall, upon request, make a summary of its policy available to the District.

3.1.1. The Vendor shall ensure that any subcontractor, service provider, or third party with access to Customer Data is contractually bound by equivalent or stronger data protection, confidentiality, and incident response obligations as outlined in this Agreement. The Vendor shall remain fully responsible for any acts or omissions of such third parties in connection with the handling of Customer Data.

3.2. At the District's request, and where such assistance is not unduly burdensome, the Vendor shall provide reasonable cooperation and support for any investigation, regulatory inquiry, or litigation arising out of or relating to the Data Incident, including support in notifying affected individuals and interfacing with regulatory authorities.

3.3. The Vendor shall not disclose the existence or details of a Data Incident to any third party, including media, regulators, or other customers, without the District's prior written approval, except as strictly required by law.

3.4. In no event shall the District be held financially liable for any costs, damages, regulatory penalties, or legal expenses arising from a breach of Customer Data caused, in whole or in part, by the Vendor, its subcontractors, or affiliates. The Vendor shall be solely responsible for all costs associated with investigation, response, notification, remediation, credit or identity monitoring, and any regulatory or legal actions stemming from such a breach.

3.5. The Vendor shall fully indemnify, defend, and hold harmless the District from and against any and all claims, damages, liabilities, penalties, costs, and expenses (including reasonable attorneys' fees) arising from or related to a Data Incident caused, in whole or in part, by the Vendor, its subcontractors, or agents. This includes, but is not limited to, costs associated with breach notification, regulatory inquiries, litigation, and third-party claims.

Service Provider Signature

Claire McAreavey

Date Signed

09/02/2026 04:56 pm

This Agreement constitutes the entire understanding among the Parties with respect to the subject matter hereof and supersedes all prior agreements, whether written or oral. No amendment or modification of this Agreement shall be valid unless in writing and signed by authorized representatives of both Parties.

As an authorized representative of my organization, I accept the conditions listed in this document.

Authorized Representative Signature

Claire McAreavey

Service Provider

Date

09/02/2026 09:26 am

Roseville City School District

Date

09/02/2026 04:57 pm

Service Provider

Name

Laura Assem

Roseville City School District

Name

Claire McAreavey

Service Provider

Title

Executive Director, Technology

Roseville City School District

Title

Head of Legal

Service Provider

Email (Service Provider)

c.mcareavey@everway.com

Service Provider

axiom worknest

EVERWAY- PEN TEST- READ&WRITE

Attestation: WEB APPLICATION ASSESSMENT

Prepared for: Everway

Date: 2026-06-03

Protective Marking: Company Confidential

Table of Contents

Disclaimer 3

Overview 4

Assessment Scope 6

Management Summary 7

Appendices 12

Web Application Assessment

Prepared For: Everway

Date of Report: 03rd June, 2026

Protective Marking: Company Confidential

Author Name: Jack Mason, Jack Mason

Author Email: jackmason@worknest.com, jackmason@worknest.com

Disclaimer

The information, representations, statements, opinions, and proposals contained in this document are provided in good faith and are believed to be accurate at the time of writing. However, they are not intended to be, and should not be construed as, legally or contractually binding unless and until incorporated into a separate written agreement executed by the relevant parties.

Any future agreement arising from discussions in connection with this document will be subject to further negotiation and agreed terms and conditions.

Unless otherwise governed by a written confidentiality agreement between the parties, this document contains confidential information belonging to the disclosing party and the recipient. Such information must not be disclosed to any third party without prior written consent from the disclosing party.

Overview

Security testing services were conducted for Everway in line with the scope of work outlined in this report. The engagement included the following activities:Web Application Assessment

Assessment Purpose

The purpose of the assessment is to identify any software or configuration vulnerabilities that could be exploited by an attacker. This includes, (but is not limited to) outdated software packages, SSL/TLS configuration issues, weak authentication controls, weak input validation controls, lack of output encoding, lack of security headers, information disclosure issues, business logic problems.

Background, Context and Drivers

Given the nature of Everway's business, it is necessary for them to store and process clients' information. It is critical that this highly sensitive information be secured through an ongoing defence in depth approach. This assessment forms part of a larger security project, ensuring that any vulnerabilities associated with the web application assessment are identified and remediated.

Caveats

The following assessment caveats were adhered to:

1. Denial-of-service attacks should not be attempted.
2. Any exploitation code known to potentially cause disruption should not be used.
3. Any automated password attacks that could lock out user accounts should not be attempted.

About this Report

This security assessment report is divided into the following sections:

Management Summary

This section provides a high-level overview of the assessment results, enabling readers to quickly understand the overall outcome. It summarises the key findings, including a brief description and associated risk level. Where appropriate, commentary is included to explain the significance of the findings, their potential business impact, and recommended remediation actions.

Detailed Technical Results

This section forms the main body of the report and contains detailed information for each identified finding. Vulnerabilities are described with supporting evidence where applicable (such as screenshots or tool output), risk ratings, remediation guidance, relevant references, and affected systems. Findings identified through both automated and manual testing techniques are included. Informational observations or non-critical issues may also be documented where relevant.

Additional Information

Supporting material that is too extensive or supplementary for inclusion in the main body of the report is provided in this section. This may include extended tool output, enumerated data, configuration extracts, or other collected evidence. Where relevant, references to this material are provided within the detailed findings.

Appendices

This section contains background information relevant to the report but not directly related to specific findings. Examples may include details of the risk rating methodology, testing approach, scope considerations, limitations, or descriptions of tools and techniques used during the assessment.

Assessment Scope

The following assessment scope was submitted by the client and confirmed during the initial briefing with the associated consultant(s). Authorisation to perform security testing on the supplied scope has been supplied and documented in the required authorisation form(s) signed by the client.

Targets

Web Application Assessment

Name	Hostname	IP Address	URL
Read&Write Chrome Extension			https://chromewebstore.google.com/detail/readwrite-for-google-chro/inoeonmfapjbbkmdafoankkfajkcphgd

Out of Scope

All testing was conducted within the limits of the scope supplied above, mitigating the risk of any breach of the 'Computer Misuse Act 1990'. The client did not provide any additional hosts within the supplied ranges that should be specifically excluded from the scan.

Management Summary

This section includes a high-level paragraph summarising the overall results of the assessment, allowing readers with little time to gain an understanding of the 'bottom line'. The key findings with a short description and level of risk are included also. The consultant's comments further explain the results of each test, their business impact and the recommended remediation steps specific to the client.

High Level Conclusion

The assessment of the Chrome extension revealed a moderate security posture, with the consultant unable to compromise any user data or exploit the extension in a way that could maliciously affect other users. However, the consultant did discover several ways to abuse the Chrome extension for personal gain. These included bypassing the free tier and using the company's AI features outside of the extension. The biggest risk to the company is the abuse of the services it provides. The consultant was able to read the API keys and tokens, enabling them to use Everway's paid AI services outside of the extension. Given the global nature of these features, abuse could result in a substantial bill running into thousands of pounds, and could potentially cause a Denial of Service situation by exhausting the AI rate limits for other users. This report details what was assessed, along with the improvements that can be made to further secure the Chrome extension.

Vulnerability Totals

Assessment Name	CRITICAL	HIGH	MEDIUM	LOW	INFO
Web Application Assessment	0	0	2	2	1

Key Points

The following list contains the key results of the tests. It should be noted that this list is not exhaustive, only containing the key points that the consultant deemed specifically significant.

Severity	Title	Description
MEDIUM	**Hardcoded Shared Credentials**	The product authenticates its entire cloud feature set, including text-to-speech, grammar checking, word prediction and translation, using static shared credentials embedded in the client-side JavaScript shipped to every install, with no per-user authentication or server-side validation. Testing confirmed these credentials can be extracted and replayed from an arbitrary origin with no login, letting anyone consume the vendor's paid AI services at its expense and exhaust the shared quota, denying these features to legitimate users.
MEDIUM	**Client-Side Licence Bypass**	Feature and market entitlement is enforced entirely on the client, derived from a plaintext, user-editable local store that carries no signature or integrity protection. The consultant demonstrated that editing this state flips a freemium account to premium and switches the market from education to workplace, with the change persisting across restarts and no server-side re-validation. Offline features unlock fully, allowing users to self-provision premium and workplace capabilities at will and circumvent commercial licensing controls.

Severity	Title	Description
LOW	**Extension Hardening**	Two content-script message handlers, injected across all visited pages, act on incoming messages without validating their origin or source, so any website the victim visits can silently and persistently reset the user's accessibility settings or pollute the diagnostic error log. Separately, the MV3 manifest declares unused and overbroad permissions and exposes web-accessible resources to all origins, widening the attack surface available to a malicious page and allowing reliable fingerprinting of the extension's presence.

Remediation Summary

This section contains a high-level summary of the remediation advice contained within this report. However, it should not be used as an exhaustive list of all required steps to resolve all security issues. Its purpose is to provide a simple view of the most significant remediation steps listed in the order of their potential to reduce vulnerabilities and improve overall security. All remediation steps can be found in the Detailed Technical Results Section below.

Severity	Title	Remediation
MEDIUM	**Enforce Server-Side Authentication**	Treat all listed credentials as compromised and rotate them, recognising that any replacement shipped in the bundle is equally extractable. Authenticate every cloud call per user using the existing licence or session token and validate it server-side on every request. Replace Access-Control-Allow-Origin: * with a server-side origin allowlist restricted to the official extension origin, apply an equivalent origin check to the ElevenLabs proxy WebSocket, and enforce per-user and per-source rate limiting and quota caps so cost is bounded.
MEDIUM	**Sign and Server-Validate Entitlements**	Stop trusting the local entitlement store and issue a license state as a signed token using an asymmetric scheme such as RS256 or Ed25519, with the private key held only by the licensing service and the signature verified on every load. Enforce entitlement for all cloud-backed features server-side rather than relying on client-supplied values, require periodic online re-validation for offline features within a defined grace period, and treat any enterprise managed-policy market value as authoritative over local storage.

Severity	Title	Remediation
LOW	**Harden Messaging and Manifest**	Validate event.origin and event.source in both message handlers before acting, remove the forgeable hashCode check, and route privileged actions such as settings resets through the extension's own runtime messaging rather than page-context messages, with user confirmation before defaults are restored. Apply least privilege to the manifest by removing the unused activeTab and management permissions, narrowing web-accessible resources to the origins that need them with dynamic URLs, removing the development origin, and setting a minimum Chrome version.

Appendices

Information associated with the report (but not directly with the specific results of the assessment) will be placed in this section. For example, explanations of the vulnerability risk rating system, testing methodology and descriptions of testing tools may be found here.

Appendix A - Risk Ratings

The table below outlines the security risk rating system used within this report.

The vulnerability rating methodology is based on the Common Vulnerability Scoring System (CVSS) version 3.0, alongside professional judgement following consideration of all relevant testing factors. As a result, the same vulnerability may receive different ratings in different environments depending on contextual risk.

Severity	CVSS	Description
CRITICAL	9.0 - 10.0	These issues should be resolved as a top priority and are often reported to the client immediately once identified. Critical rated issues are those that are highly likely or are certain to result in a complete loss of confidentiality, integrity or availability. These issues would include those that allow a consultant (or an attacker) to compromise a target host or service.
HIGH	7.0 - 8.9	These issues should be resolved as a priority, typically being associated with unsupported software versions or services known to have serious vulnerabilities that may potentially have publicly available exploitation scripts.

Severity	CVSS	Description
MEDIUM	4.0 - 6.9	These issues are those that could potentially lead to a full breach of security but are of a lower risk. For example, a vulnerability that can be identified but for which there is no publicly available exploitation script, or a vulnerability that's exploitation requires a series of unlikely variables to exist, or a vulnerability that can be used to enumerate corporate information deemed as partially sensitive.
LOW	0.1 - 3.9	These issues are those that do not present any immediate threat, but do still present a security issue. These typically include vulnerabilities that disclose partially sensitive information.

Everway

EVERWAY RESPONSIBLE Al & DATA PROTECTION FRAMEWORK

Privacy-First Artificial Intelligence for Educational Excellence

Version: 2.1

Effective date: November 2025

Classification: Public - Customer Disclosure

Executive Summary

Everway is committed to enhancing educational outcomes with Al while maintaining high standards of privacy, security, and ethics. This Framework sets out our governance and data-protection approach to ensure Al serves educational purposes, built on an architecture where Al components do not access or process identifiable personal data

Core Data Protection Commitment: Everway's Al components are designed to avoid accessing, processing, or retaining personal data by default. Personal data processed elsewhere in the service (e.g., authentication, support, audit) remains subject to strict controls. Where identifiable personal data is present or reasonably expected, it is redacted and pseudonymized before transfer to third-party Al providers. All data is strictly excluded from third-party Al model training.

---

1. Fundamental Principles

1.1Privacy by Design and Default

- Data minimization protocols are embedded in system architecture.
- Automatic redaction and pseudonymization layers are applied prior to Al processing in accordance with our technical protocols and privacy risk assessments.
- Where aggregation or anonymization is claimed, we document the technique and re-identification risk assessment.
- Personal identifiers are systematically redacted or pseudonymized within Al training datasets in accordance with our technical protocols
- Privacy impact assessments are conducted for new Al implementations or for major updates that materially change data processing or risk profile.

1.2 Human-Centered Al

- Al augments, not replaces, human judgment, creativity, or decision-making.
- Mandatory human oversight is required for Al outputs that may materially influence pedagogy, learning feedback, or student progression. Low-risk assistive outputs follow risk-based review and sampling.
- Educator control over Al assistance features is maintained, and student agency is supported via opt-in mechanisms.

- User interfaces are designed to distinguish between AI-generated suggestions and human decision-making.

1.3 Transparency & Explainability

- We provide plain-language explanations of AI system operations.
- Clear disclosure is provided when a user is interacting with an AI system, either within the product interface or through accessible documentation (e.g., Data Packs), proportionate to the feature's function.
- Documentation regarding capabilities and limitations (e.g., Model Cards) is maintained for proprietary AI models. For third-party GenAI services, we reference vendor-provided system cards.
- For proprietary AI models, performance metrics are monitored internally as part of our standard operational maintenance procedures.

1.4 Fairness & Non-Discrimination

- Bias detection and mitigation protocols are established and implemented as part of our risk-based AI lifecycle.
- Regular fairness audits are conducted using appropriate methodologies (such as proxy data analysis or outcome testing) to test for biased outcomes.
- Inclusive design processes involve input from diverse stakeholders.
- Ongoing monitoring is performed as part of the operations phase to detect potential discriminatory patterns.

1.5 Safety & Security

- Threat modelling and risk assessment are conducted for new AI systems and major updates.
- AI development is governed by our existing ISO-certified Secure Development Lifecycle (SDLC). We apply risk-appropriate security reviews, such as architectural threat modeling and fairness assessments, to ensure AI systems meet our safety standards prior to deployment.
- Our AI components are included within the scope of our periodic security audits and penetration tests. AI-specific vulnerability testing is conducted as determined by our risk assessment process.
- AI-specific incident response procedures are in place.

1.6 Accountability & Governance

- A designated AI Ethics Board provides oversight (see Section 7).
- Clear roles and responsibilities for AI governance are defined.
- Regular internal and external audits are conducted.
- Key AI-related decision-making processes are documented.

---

2. AI System Architecture & Data Handling

Everway

2.1 AI System Categories

Our framework governs all AI systems, which fall into two primary categories:

- **Internal AI Systems:** These are systems developed and operated by Everway. They are architecturally isolated from identifiable personal data and operate only on anonymized or pre-approved, non-personal content.
- **Third-Party AI Services:** Data transfer is governed by a risk-based control framework. While our primary standard is to process data through a redaction and pseudonymization gateway, low-risk functional services (e.g., text-to-speech) may operate under strict contractual isolation without a gateway, provided they do not retain data or use it for model training.

2.2 Data Classification & Handling

The table below defines what data our AI models are permitted to process after it has passed through our secure anonymization gateway.

Data type	AI Model Processing (Post-Gateway)	Examples	Safeguards
Non-Personal Data	Yes	Course templates; question banks; anonymized research data.	Data does not relate to an identifiable person.
Anonymized or Pseudonymized User Data	Yes	"User 451 answered topic X incorrectly"; "User 789's score was 80%."	No user identifiers are processed by the AI models.

PII (Personal Data)	**No**	"Names, emails, IDs."	Processed by the anonymization gateway or protected via strict contractual isolation and input controls (see Section 2.3).
Biometric data	No	"Voice, face."	Prohibited by policy.

2.3 Technical Safeguards

- Architectural isolation of AI processing systems from personal-data stores.
- A redaction and pseudonymization gateway is the primary standard for AI processing. For real-time features where a gateway is not utilized, we rely on strict vendor contractual protections (prohibiting model training). In these instances, privacy is maintained either through explicit user warnings or by the functional nature of the tool (e.g., processing non-personal academic content), which limits the likelihood of personal data submission
- Sufficient audit logging is maintained for AI system operations to ensure security, compliance, and incident response.
- Encryption: TLS 1.3 for data in transit; AES-256 for data at rest.
- Role-based access controls based on the principle of least privilege.

---

3. Compliance & Regulatory Alignment

3.1 EU AI Act

- Based on current features, our AI systems are assessed as Limited Risk under the EU AI Act. We do not perform biometric categorization, emotion inference, social scoring, or remote biometric identification. We meet transparency obligations (Art. 52) and apply proportionate risk controls.
- **Measures:** We implement measures aligned with the Act, including Article 4 (AI literacy programs), Article 5 (prevention of prohibited practices), transparency obligations, documentation and logging requirements, and mandatory human oversight.
- **GPAI usage:** When utilizing General-Purpose AI models, we review vendor copyright indemnification and compliance assurances, reference vendor-provided system cards, and conduct risk assessments to ensure alignment with our responsible AI governance standards.

3.2 US Federal Laws

Our framework is designed to support FERPA, COPPA, and CIPA compliance in partnership with schools and districts. We provide configuration controls, DPA terms, and documentation; ultimate compliance often depends on customer deployment choices.

- **FERPA:** Identifiable education records are not processed by AI systems. All such data is protected via pseudonymization or strict contractual provisions prohibiting data retention and model training. Directory information is not intended for AI processing and is subject to our standard redaction protocols.
- **COPPA:** We do not use identifiable personal data from children under 13 for AI processing. Any such data is protected via pseudonymization or strict contractual isolation before it is used by an AI component. Appropriate consent (via verifiable parental consent or authorized school consent under COPPA) is required for AI features targeting children, and no training occurs on children's data.
- **CIPA:** Our AI systems are architected to support CIPA requirements. Content filtering, where applicable, is managed in accordance with our AI-specific security architecture (see 12.2) and operational monitoring procedures (see 4.3), and monitoring capabilities are used without retaining personal data
- **SOPPA (Student Online Personal Protection Act):** We comply with Illinois' SOPPA requirements by ensuring privacy and security of student data collected through educational technology services. This includes entering into compliant data privacy agreements with schools, collecting only necessary information, using student data solely for educational purposes, and not selling or sharing it for marketing. We implement strong security measures to protect data from unauthorized access and allow schools and parents to review, correct, or delete student information as required. Our redaction and pseudonymization protocols ensure AI systems do not process identifiable student data. Regular audits and transparency about data practices further support SOPPA compliance.

3.4 Canadian Privacy Laws

PIPEDA (Personal Information Protection and Electronic Documents Act): Our framework aligns with PIPEDA's requirements for how private-sector organizations collect, use, and disclose personal information in commercial activities. Our AI architecture inherently supports PIPEDA compliance through data minimization and our zero personal-data processing approach.

Measures: We implement PIPEDA-aligned practices including obtaining appropriate consent for data collection, limiting data collection to what is necessary for identified purposes, securing personal information through encryption and access controls, providing individuals with access to their personal information, and maintaining Data Processing Agreements that govern cross-border data transfers.

Provincial Laws: We maintain awareness of provincial privacy legislation including British Columbia's Personal Information Protection Act (PIPA) and Quebec's Law 25, which impose

additional requirements such as designated privacy officers, privacy impact assessments for sensitive projects, and mandatory breach notification to authorities and affected individuals.

3.5 Australian Privacy Laws

Privacy Act 1988: Our framework is designed to comply with the Australian Privacy Principles (APPs) contained in the Privacy Act 1988. Our AI systems' architecture supports compliance by design through our data minimization approach and privacy-preserving technical safeguards.

Measures: We align with the APPs through practices including transparent privacy policies, purpose limitation for data collection and use, data quality and security measures, providing individuals with access and correction rights, and cross-border disclosure safeguards for any third-party AI services. Our redaction and pseudonymization gateway ensures that AI processing does not involve identifiable personal information, supporting compliance with sensitive information handling requirements.

3.6 New Zealand Privacy Laws

Privacy Act 2020: Our framework complies with New Zealand's enhanced Privacy Act 2020, which strengthens protections for personal information. The Act's 13 privacy principles align closely with our existing privacy-by-design approach.

Measures: We support Privacy Act 2020 compliance through data security safeguards, mandatory breach notification procedures, privacy impact assessments for new AI systems, transparency about AI data handling practices, and mechanisms for individuals to access, correct, and request deletion of their personal information. Our architectural separation of AI systems from personal data stores inherently supports the Act's requirements for appropriate personal information handling.

---

4. AI Lifecycle Management

4.1 Development Phase

- **Requirements:** The development process includes a risk-based assessment of educational impact, privacy, and ethics. Stakeholder consultations are conducted as appropriate.
- **Design:** Incorporates privacy-preserving patterns, defines explainability requirements, and includes bias prevention measures.
- **Development/Testing:** Follows our standard ISO secure coding practices, including testing for edge cases.

4.2 Deployment Phase

- **Pre-Deployment Reviews:** Requires AI Ethics Board review and approval, proportionate to the system's risk, including compliance verification, risk assessment, and documentation review.
- **Deployment Controls:** Uses a controlled process including monitoring and feedback collection. Where appropriate to the risk and scale of the change, this process may also include gradual rollouts, A/B testing, and performance baseline establishment.

4.3 Operations Phase

- **Monitoring:** Includes ongoing performance monitoring, drift detection for AI models, and adherence to monitoring-informed retraining schedules.
- Incident response procedures are in place.
- **User Support:** Provides AI literacy resources, clear opt-out mechanisms, feedback channels, and clear support documentation.

4.4 Retirement Phase

- **Decommissioning:** Follows formal data deletion protocols, maintains model retirement documentation, executes user notification processes, and provides alternative solutions where applicable.

---

5. Ethical Considerations

5.1 Educational Ethics

- Pedagogical Integrity: AI supports but does not replace established educational methodologies.
- We focus on preserving critical thinking, creativity, academic integrity, and ensuring age-appropriate AI interactions.
- Digital Equity: We consider varying levels of digital access, ensure alternative non-AI options are available for core services, support diverse learning needs, and target accessibility compliance (WCAG 2.1Level AA).

5.2 Algorithmic Accountability

- **Bias Prevention and Mitigation:** Our accountability process includes a risk-based approach to bias prevention. As appropriate, this may include pre-deployment testing, fairness audits, strategies for using diverse data, and ongoing monitoring for emergent biases.
- **Explainability:** We are committed to transparency. This includes providing user-friendly explanations for AI recommendations where appropriate, documenting decision logic proportionate to its impact, offering channels for users to report or contest material AI outputs, and being transparent about system limitations.

5.3 Environmental Responsibility

- **Sustainable AI:** We strive to use energy-efficient model architectures, monitor the carbon footprint of our AI operations, optimize for computational efficiency, and give preference to green computing infrastructure where feasible.

---

6. User Rights & Controls

6.1 Fundamental Rights

- **Right to Information:** Users receive clear notification when interacting with AI systems and accessible explanations about their function, proportionate to the feature's impact.
- **Right to Human Review:** Users have a channel to request human review of material AI recommendations.
- **Right to Opt-Out:** Everway provides AI opt-out where feasible without materially degrading the contracted service. For AI-inclusive products, AI functionality is intrinsic to the service and may be required for core workflows. In these cases, Everway provides: (a) upfront disclosure that AI is essential to the product; (b) role-appropriate user control over when AI suggestions are applied to a record or submitted; and (c) strong data minimization, privacy, and oversight controls. Customers who require AI-disabled operation should procure a non-AI alternative product or use documented export workflows.

6.2 Consent Management

- **Consent:** Our consent processes are designed to be explicit and specific, proportionate to the AI feature's risk and context.
- We aim to provide simple withdrawal mechanisms and age-appropriate consent processes.
- **Parental Controls:** Our platform supports parental controls, which may include consent mechanisms, AI feature settings, and educational resources.

6.3 GDPR Data-Subject Rights (Context: AI does not process personal data)

While Everway's AI architecture is designed to avoid processing identifiable personal data, we uphold the spirit of GDPR rights:

- We are committed to information transparency regarding AI operations.
- We provide mechanisms for users to request rectification of any system errors.
- We honor the Right to Erasure. This is straightforward for our AI systems, as they do not retain personal data. Upon a valid request, we will erase personal data from all our systems, including your core account records, in accordance with regulatory requirements.
- The right to object is implemented via our opt-out mechanisms.
- Human intervention is available for AI-assisted processes that materially influence pedagogy or assessment, consistent with our human oversight principles (see 1.2).

---

7. Governance Structure

7.1 AI Ethics Board

- **Composition:** The board is chaired by a designated AI executive and includes senior representatives from key functions, including Compliance ,Technology, Legal, and Education. It also includes both internal and external ethics advisors and stakeholder representatives as appropriate.
- **Responsibilities:** Responsibilities: Review and approve business requests for AI feature inclusion in products; provide oversight and approval for new AI implementations proportionate to their risk; guide ethical compliance; address stakeholder concerns; advise on policy development; review audit findings; and oversee the development and delivery of AI literacy and stakeholder training programs.

7.2 Operational Governance

- **AI Product Management:** Responsible for day-to-day AI system operations, implementing board decisions, performance monitoring, and initial incident response.
- **Compliance Function:** Handles regulatory monitoring, conducts compliance assessments, maintains documentation, and coordinates audits.
- **Education & Support Function:** Responsible for creating user support materials, developing AI literacy resources for customers, and integrating user feedback.
- **Legal:** Reviews vendor Master Service Agreements (MSAs) and Data Processing Agreements (DPAs) for AI services, provides counsel on regulatory requirements, and supports contract negotiations to ensure compliance with privacy and data protection standards.

7.3 External Oversight

- **Audits:** AI systems and processes are included within the scope of our Internal Audit Program. AI is currently within the scope of our ISO 27001external audit (BSI). Should ISO 42001 certification be pursued in future, AI would be added to that external scope.
- Audit summaries are made available to stakeholders upon request.
- **Advisory Council:** Periodic reviews occur with external experts to integrate industry best practices, identify emerging risks, and provide strategic guidance.

---

8. Incident Response & Remediation

8.1 Classification Matrix

Severity	Description	Response Target	Escalation Path

Critical	Harmful/discriminatory AI output	Immediate Triage	Immediate escalation to AI Governance Lead and Legal, who coordinate the response and engage executive leadership as appropriate.
High	Significant bias or privacy concern	Triage Target: < 2 hours	AI Governance Lead, Compliance (DPO), and Legal
Medium	Performance degradation/user complaints	Triage Target:< 24 hours	AI Product Team
Low	Minor issues/enhancements	Triage Target:< 72 hours	Standard process

8.2 Procedures Our incident response procedures follow a standard, risk-based methodology:

1. **Triage & Containment:** Involves immediate assessment of the report, isolation of the system if necessary, and escalation to the appropriate team based on severity.
2. **Investigation & Remediation:** Involves conducting a root-cause analysis proportionate to the incident, implementing corrective actions, and validating the fix.
3. **Post-Incident Review:** For significant incidents, a post-incident review is conducted to document lessons learned, assess the need for process improvements, and communicate with stakeholders as appropriate.

---

9. Continuous Improvement

9.1 Metrics

- **We track key performance and risk metrics for our AI systems.** These metrics may include, as appropriate, technical accuracy, system availability, educational efficacy, user satisfaction, and compliance adherence.

9.2 Review Cycles

- **We conduct periodic reviews** of AI system performance, risk, and user feedback. This framework is reviewed at least annually, or as needed to respond to new technologies, regulations, or business needs.

9.3 Innovation Framework

- **Process:** Our innovation process is guided by responsible, privacy-preserving principles, from idea generation to deployment and optimization.
- **R&D:** Our R&D activities may include collaborations with academic institutions, participation in industry standards bodies, and contributing to responsible AI research.

---

10. Stakeholder Engagement

10.1 Communication

- **Internal:** We are committed to internal awareness through periodic AI updates to staff, role-based training, and maintaining feedback channels.
- **External:** We engage with our customers and stakeholders through mechanisms such as transparency reports, customer feedback forums, and participation in public policy discussions..

10.2 Education & Training

- **Staff:** We provide mandatory AI literacy training for relevant staff, supplemented by role-specific advanced training. We focus on ethical decision-making and continuous learning opportunities.
- **Customers:** We support our customers with resources such as feature guides, tutorials, and best practice recommendations to promote safe and effective AI use.

10.3 Feedback Mechanisms

- We maintain multiple channels for feedback, which may include in-product tools, surveys, and community forums.
- Feedback is systematically categorized, prioritized, and reviewed to help inform the product roadmap.

---

11. Regulatory Compliance Matrix

11.1 Mapping

Regulation	Requirement	Implementation	Validation

EU AI Act Art. 4	AI literacy	Comprehensive training	Records & assessments
EU AI Act Art. 5	Prohibited practices	Technical/policy controls	Audits & monitoring
EU AI Act Art. 52	Transparency	AI interaction notices	UI review
GDPR Art. 22	Automated decisions	AI is not used for automated decisions that produce legal or similarly significant effects.	Architecture review
FERPA	Education records privacy	Pseudonymization or strict contractual isolation	Data-flow analysis
COPPA	Children's privacy	PII pseudonymized/anonymized before AI processing	PIA reviews
1S042001	AI Mgmt. System	Comprehensive AIMS	Aligned (Self-Assessed)
NIST AI RMF	Risk management	Integrated framework	Risk assessments

11.2 Regulatory Monitoring

- We utilize a process to monitor regulatory updates, which includes inputs from legal counsel and industry associations.
- Our adaptation process involves assessing the impact of new regulations, planning for implementation, and verifying compliance.

12. Technical Specifications

12.1 AI Model Governance

We maintain an internal inventory of our AI models and systems.
This inventory is used to manage risk, guide our review processes, and ensure oversight is applied proportionate to the model's function and risk level.

12.2 Security Architecture

- We apply a defense-in-depth security model to our systems.
- Our AI components are protected by a robust set of technical and procedural controls designed to protect against common and emerging threats.
- These controls include, where appropriate, network segmentation, access controls, encryption, and regular security assessments. We follow AI-specific secure-coding and validation practices to mitigate risks such as prompt-injection and model manipulation

12.3 Data Architecture

- **Privacy-preserving techniques:** Our primary technique is our Privacy-by-Design architecture. Identifiable personal data is primarily processed by a secure, isolated gateway. For real-time features where a gateway is not utilized, we rely on strict vendor contractual protections (prohibiting model training) alongside context-appropriate safeguards. Our AI models are only trained on, and only process, data that does not contain personal identifiers, such as pre-approved content and fully anonymized action patterns.

13. Third-Party AI Services

13.1 Vendor Management

- **Selection:** We use a risk-based due diligence process to select third-party AI vendors, assessing their privacy, security, and ethical practices. Legal reviews all vendor MSAs and DPAs to ensure contractual protections align with our framework requirements.
- **Ongoing:** We conduct periodic reviews of vendor performance and compliance, proportionate to the service's risk.

13.2 Data Processing Agreements (Required)

- We require Data Processing Agreements (DPAs) with our AI vendors. These agreements are designed to govern data use, prohibit unauthorized model training, and require that data is protected in line with our policies and regulatory requirements.

13.3 Risk Management

- Our vendor risk management process includes initial evaluation, ongoing monitoring proportionate to the vendor's risk, and contingency planning.

---

14. Continuous Evolution

- We are committed to the periodic review and continuous evolution of this framework. This ensures our practices remain aligned with emerging technologies, stakeholder feedback, and regulatory requirements. We will remain transparent about significant changes and continue to engage with our stakeholders to maintain leadership in responsible AI for education.

Appendices

- **AI System:** Any system that uses artificial intelligence techniques including machine learning, natural language processing, or rule-based systems.
- **Personal Data/PII:** Any information relating to an identified or identifiable natural person.
- **Model Card:** Documentation providing details about an AI model's intended use, limitations, and performance metrics.
- **Pseudonymization:** The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information.
- **Redaction:** The process of masking or removing personal data from a dataset.

Appendix B: Revision History

- v2.0 (Oct 2025): Complete rewrite aligned with current regulations and standards.
- v1.0: Initial framework.

Appendix C: Certifications & Compliance Status

- ISO/IEC 42001 (AI Management System): In Progress
- ISO/IEC 27001:2022 (, Information Security): Certified
- SOC 2 Type II (Security, Availability, Confidentiality): Aligned
- EU AI Act/ GDPR / FERPA /COPPA/ State Laws: **Aligned** (Self-Assessed based on framework implementation)

Appendix D: AI Literacy Curriculum Outline Our AI literacy training is role-based and includes:

- **Foundation (relevant staff): Includes** AI fundamentals, ethics, privacy/security, and an overview of Everway principles and regulations.

Everway

- **Advanced (technical & product roles): Includes topics such as** privacy-preserving architecture, risk assessment, and bias mitigation.
- **Leadership: Includes topics such as** governance, regulatory strategy, and ethical decision-making.

Attestation

This Responsible AI & Data Protection Framework represents Everway's unwavering commitment to protecting user data while leveraging ethical, transparent artificial intelligence in education. We pledge to maintain our zero personal-data architecture and continuously improve our practices to serve the best interests of students. educators, and institutions worldwide.

Approved by:

EVP of AI

Everway

Date: November 2025

Chief Executive Officer

Everway

Date: November 2025

Chief Technology Officer

Everway

Date: November 2025

Chief Information Officer

Everyway

Date: November 2025

This document may be shared with customers, partners, and regulators as part of Everway's commitment to transparency in AI governance.

For the most current version of this framework, please visit everway.com/responsible-ai.

Everway

Everway

Everway Privacy Policy

Last updated December 20, 2024

This Privacy Notice for Everway, and its entities ("**we**," "**us**," or "**our**"), describes how and why we might access, collect, store, use, and/or share ("**process**") your personal information when you use our services ("**Services**"), including when you:

- Visit our website at http://www.everway.co, or any website of ours that links to this Privacy Notice
- Engage with us in other related ways, including any sales, marketing, or events
- It also contains information about your choices and privacy rights

Questions or concerns? Reading this Privacy Notice will help you understand your privacy rights and choices. If you still have any questions or concerns, please contact us at dataprotection@texthelp.com.

Our services

This summary provides key points from our Privacy Notice, but you can find out more details about any of these topics by clicking the link following each key point or by using our table of contents below to find the section you are looking for.

This Privacy notice does not apply to:
(i) the data we process on behalf of our customers (where we act as a data processor), this is addressed by our agreements with our customers;
(ii) personal information that we collect in connection with our products, this is addressed in our Product Privacy Notice
(iii) personal information that we collect and process in connection with our recruitment activities, which is covered under our Employees, Contractors, Applicants Privacy Notice.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and the products and features you use. Learn more about personal information you disclose to us.

Do we process any sensitive personal information? Some of the information may be considered "special" or "sensitive" in certain jurisdictions, for example your racial or ethnic origins, sexual orientation, and religious beliefs. We may process sensitive personal information when necessary with your consent or as otherwise permitted by applicable law. Learn more about sensitive information we process.

Do we collect any information from third parties? We may collect information from public databases, marketing partners, social media platforms, and other outside sources. Learn more about information collected from other sources.

Everway

How do we process your information? We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so. Learn more about how we process your information.

In what situations and with which parties do we share personal information? We may share information in specific situations and with specific third parties. Learn more about when and with whom we share your personal information.

How do we keep your information safe? We have adequate organizational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Learn more about how we keep your information safe.

What are your rights? Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information. Learn more about your privacy rights.

How do you exercise your rights? The easiest way to exercise your rights is by completing the Data Subject Access Request/Data Deletion Request Form or by contacting us at dataprotection@texthelp.com. We will consider and act upon any request in accordance with applicable data protection laws.

Want to learn more about what we do with any information we collect? Review the Privacy Notice in full.

Table of contents

1. What information do we collect?

2. How do we process your information?

3. What legal bases do we rely on to process your personal information?

4. When and with whom do we share your personal information?

5. Do we use cookies and other tracking technologies?

6. Do we offer artificial intelligence-based products?

7. How do we handle your social logins?

8. How long do we keep your information?

Everway

9. How do we keep your information safe?

10. Do we collect information from minors?

11. What are your privacy rights?

12. Controls for do-not-track features

13. Do United States residents have specific privacy rights?

14. Do other regions have specific privacy rights?

15. Do we make updates to this notice?

16. How can you contact us about this notice?

17. How can you review, update, or delete the data we collect from you?

1. What information do we collect?

Personal information you disclose to us

In Short: *We collect personal information that you provide to us.*

We collect personal information that you provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us. See 'Section 2 - How do we process your information' for further details.

Personal information provided by you. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect include the following:

- names
- phone numbers
- email addresses
- mailing addresses
- job titles
- billing addresses
- contact preferences

Sensitive information. When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:

- Financial data

Payment data. We may collect data necessary to process your payment if you choose to make purchases, such as your payment instrument number, and the security code associated with your payment instrument. All payment data is handled and stored by our Payment Providers Stripe and Authorize.net. You may find their privacy notice link(s) here: https://stripe.com/gb/privacy and https://www.visa.co.uk/legal/global-privacy-notice.html.

Social media login data. We may provide you with the option to register with us using your existing social media account details, like your Facebook, X, or other social media account. If you choose to register in this way, we will collect certain profile information about you from the social media provider, as described in the section called "How do we handle your social logins?" below.

All personal information that you provide to us must be true, complete, and accurate.

Information automatically collected

In Short: *Some information — such as your Internet Protocol (IP) address and/or browser and device characteristics — is collected automatically when you visit our Services.*

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes.

Like many businesses, we also collect information through cookies and similar technologies. You can find out more about this in our Cookie Notice: https://www.everway.co/cookies/.

The information we collect includes:

- *Log and usage data.* Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called "crash dumps"), and hardware settings).
- *Device data.* We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, Internet service provider and/or mobile carrier, operating system, and system configuration information.

- *Location data.* We collect location data such as information about your device's location, which can be either precise or imprecise. How much information we collect depends on the type and settings of the device you use to access the Services. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your IP address). You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your Location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of the Services.

Google API

Our use of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements. Please see the link to our Product Privacy Policy.

Information collected from other sources

In Short: *We may collect limited data from public databases, marketing partners, social media platforms, and other outside sources.*

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases, joint marketing partners, affiliate programs, data providers, social media platforms, and from other third parties. This information includes mailing addresses, job titles, email addresses, phone numbers, intent data (or user behavior data), Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion.

If you interact with us on a social media platform using your social media account (e.g., Facebook or X), we receive personal information about you from such platforms such as your name, email address, and gender. You may have the right to withdraw your consent to processing your personal information. Learn more about withdrawing your consent. Any personal information that we collect from your social media account depends on your social media account's privacy settings. Please note that their own use of your information is not governed by this Privacy Notice.

2. How do we process your information?

In Short: *We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.*

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To deliver and facilitate delivery of services to the user.** We may process your information to provide you with the requested service.
- **To fulfill and manage your orders.** We may process your information to fulfill and manage your orders, payments, returns, and exchanges made through the Services.
- **To send you marketing and promotional communications.** We may process the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. You can opt out of our marketing emails at any time. For more information, see "What are your privacy rights?" below.
- **To deliver targeted advertising to you.** We may process your information to develop and display personalized content and advertising tailored to your interests, location, and more. For more information see our Cookie Notice: https://www.everway.co/cookies/.
- **To protect our services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To identify usage trends.** We may process information about how you use our Services to better understand how they are being used so we can improve them.
- **To determine the effectiveness of our marketing and promotional campaigns.** We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.

3. What legal bases do we rely on to process your information?

In Short: *We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests.*

If you are located in the EU or UK, this section applies to you.

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to process your personal information:

- **Consent.** We may process your information if you have given us permission (i.e., consent) to use your personal information for a specific purpose. You can withdraw your consent at any time. Learn more about withdrawing your consent.
- **Performance of a contract.** We may process your personal information when we believe it is necessary to fulfill our
- contractual obligations to you, including providing our Services or at your request prior to entering into a contract with you.

- **Legitimate interests.** We may process your information when we believe it is reasonably necessary to achieve our legitimate business interests and those interests do not outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:
- Send users information about special offers and discounts on our products and services
- Develop and display personalized and relevant advertising content for our users
- Analyze how our Services are used so we can improve them to engage and retain users
- Support our marketing activities
- Diagnose problems and/or prevent fraudulent activities
- **Legal obligations.** We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- **Vital interests.** We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as situations involving potential threats to the safety of any person.

If you are located in Canada, this section applies to you.

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way
- For investigations and fraud detection and prevention
- For business transactions provided certain conditions are met
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle an insurance claim
- For identifying injured, ill, or deceased persons and communicating with next of kin
- If we have reasonable grounds to believe an individual has been, is, or may be victim of financial abuse
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced
- If the collection is solely for journalistic, artistic, or literary purposes
- If the information is publicly available and is specified by the regulations

Everway

4. When and with whom do we share your personal information?

In Short: *We may share information in specific situations described in this section and/or with the following third parties.*

We may need to share your personal information in the following situations:

- **Business transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.
- **Affiliates.** We may share your information with our affiliates, in which case we will require those affiliates to honor this Privacy Notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us

Sharing personal data with third parties

We also use a number of service providers to help deliver our services. These parties are subject to appropriate safeguards, in line with applicable data protection legislation.

These service providers include:

- Customer Relationship Management System (CRM) - Salesforce
- Payment Processors – to securely process your card payments (we do not see, or store payment card details)
- SMS/Email Providers – to send out our SMS/Email notifications or messages sent by Customers using Everway Products and Services - Salesforce Marketing Cloud
- Hosting Providers – to manage our secure enterprise data centers
- Security Providers – to protect our systems from attack
- Telephony Providers – we might record calls for training, quality and security purposes
- Training Platforms – to train staff on the use of our services - Docebo & Reach 360
- Support Portal – so that you can easily ask for help - Zendesk
- Cloud Hosting and Recovery – working with AWS and Azure
- Security insight and system logging – working with Rapid7
- Cloud email delivery – working with Sendgrid (USA hosted)
- Anonymous Web Analytics – working with Google
- Data centers, networking and disaster recovery

Everway also engages various third party subprocessors to support the operation of our suite of products. Those we use are listed in the Texthelp Products Processor List. All data stored by Everway is stored according to our Information Security Policy. If we need to change or add additional third parties, we will always update our Sub-Processor list accordingly.

5. Do we use cookies and other tracking technologies?

In Short: *We may use cookies and other tracking technologies to collect and store your information.*

We may use cookies and similar tracking technologies (like web beacons and pixels) to gather information when you interact with our Services. Some online tracking technologies help us maintain the security of our Services and your account, prevent crashes, fix bugs, save your preferences, and assist with basic site functions.

We also permit third parties and service providers to use online tracking technologies on our Services for analytics and advertising, including to help manage and display advertisements, to tailor advertisements to your interests, or to send abandoned shopping cart reminders (depending on your communication preferences). The third parties and service providers use their technology to provide advertising about products and services tailored to your interests which may appear either on our Services or on other websites.

To the extent these online tracking technologies are deemed to be a "sale"/"sharing" (which includes targeted advertising, as defined under the applicable laws) under applicable US state laws, you can opt out of these online tracking technologies by submitting a request as described below under section "Do united states residents have specific privacy rights?"

Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice: https://www.everway .co/cookies/.

Google Analytics

We may share your information with Google Analytics to track and analyze the use of the Services. The Google Analytics Advertising Features that we may use include: Remarketing with Google Analytics and Google Analytics Demographics and Interests Reporting. To opt out of being tracked by Google Analytics across the Services, visit https://tools.google.com/dlpage/gaoptout. You can opt out of Google Analytics Advertising Features through Ads Settings and Ad Settings for mobile apps. Other opt out means include http://optout.networkadvertising.org/ and http://www.networkadvertising.org/mobile-choice. For more information on the privacy practices of Google, please visit the Google Privacy & Terms page.

6. Do we offer artificial intelligence-based products?

In Short: *We offer products, features, or tools powered by artificial intelligence, machine learning, or similar technologies.*

As part of our Services, we offer products, features, or tools powered by artificial intelligence, machine learning, or similar technologies (collectively, "AI Products"). These tools are designed to enhance your experience and provide you with innovative solutions. The terms in this Privacy Notice govern your use of the AI Products within our Services.

Use of AI technologies

We provide the AI Products through third-party service providers ("AI Service Providers"), including OpenAI. As outlined in this Privacy Notice, your input, output, and personal information will be shared with and processed by these AI Service Providers to enable your use of our AI Products for purposes outlined in "What legal bases do we rely on to process your personal information?" You must not use the AI Products in any way that violates the terms or policies of any AI Service Provider.

Our AI products

Our AI Products are designed for the following functions:

- AI bots

Our AI service providers

- OpenAI
- Elevenlabs

How we process your data using AI

All personal information processed using our AI Products is handled in line with our Privacy Notice and our agreement with third parties. This ensures high security and safeguards your personal information throughout the process, giving you peace of mind about your data's safety.

7. How do we handle your social logins?

In Short: *If you choose to register or log in to our Services using a social media account, we may have access to certain information about you.*

Our Services offer you the ability to register and log in using your third-party social media account details (like your Facebook or X logins). Where you choose to do this, we will receive certain profile information about you from your social media provider. The profile information we receive may vary depending on the social media provider concerned, but will often include your name, email address, friends list, and profile picture, as well as other information you choose to make public on such a social media platform.

We will use the information we receive only for the purposes that are described in this Privacy Notice or that are otherwise made clear to you on the relevant Services. Please note that we do not control, and are not responsible for, other uses of your personal information by your third-party social media provider. We recommend that you review their privacy notice to understand how they collect, use, and share your personal information, and how you can set your privacy preferences on their sites and apps.

8. How long do we keep your information?

In Short: *We keep your information for as long as necessary to fulfill the purposes outlined in this Privacy Notice unless otherwise required by law.*

We will only keep your personal information for as long as it is necessary for the purposes set out in this Privacy Notice, and Everway's Data Retention Policy, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible. For more information on Everway's Data Retention periods please contact the DPO, dataprotection@texthelp.com.

9. How do we keep your information safe?

In Short: *We aim to protect your personal information through a system of organizational and technical security measures.*

We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

10. Do we collect information from minors?

In Short: *We do not knowingly collect data from or market to children under 18 years of age.*

We do not knowingly collect, solicit data from, or market to children under 18 years of age, nor do we knowingly sell such personal information. By using the Services, you represent that you are at least 18 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at dataprotection@texthelp.com.

11. What are your privacy rights?

In Short: *Depending on your state of residence in the US or in some regions, such as the European Economic Area (EEA), United Kingdom (UK), Switzerland, and Canada, you have rights that allow you greater access to and control over your personal information. You may*

review, change, or terminate your account at any time, depending on your country, province, or state of residence.

In some regions (like the EEA, UK, Switzerland, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure; (iii) to restrict the processing of your personal information; (iv) if applicable, to data portability; and (v) not to be subject to automated decision-making. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us by using the contact details provided in the section "How can you contact us about this notice?" below.

We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your Member State data protection authority or UK data protection authority.

If you are located in Switzerland, you may contact the Federal Data Protection and Information Commissioner.

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us by using the contact details provided in the section "How can you contact us about this notice?" below or updating your preferences.

However, please note that this will not affect the lawfulness of the processing before its withdrawal nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: You can unsubscribe from our marketing and promotional communications at any time by clicking on the unsubscribe link in the emails that we send, or by contacting us using the details provided in the section "How can you contact us about this notice?" below. You will then be removed from the marketing lists. However, we may still communicate with you — for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- Contact us using the contact information provided.
- Log in to your account settings and update your user account.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services. For further information, please see our Cookie Notice: https://www.everway.co/cookies/.

If you have questions or comments about your privacy rights, you may email us at dataprotection@texthelp.com.

12. Controls for do-not-track features

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Notice.

California law requires us to let you know how we respond to web browser DNT signals. Because there currently is not an industry or legal standard for recognizing or honoring DNT signals, we do not respond to them at this time.

13. Do United States residents have specific privacy rights?

In Short: *If you are a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, or Virginia, you may have the right to request access to and receive details about the personal information we maintain about you and how we have processed it, correct inaccuracies, get a copy of, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. More information is provided below.*

Categories of personal information we collect

We have collected the following categories of personal information in the past twelve (12) months:

Everway

Category	Examples	Collected
A. Identifiers	Contact details, such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol address, email address, and account name	YES
B. Personal information as defined in the California Customer Records statute	Name, contact information, education, employment, employment history, and financial information	YES
C. Protected classification characteristics under state or federal law	Gender, age, date of birth, race and ethnicity, national origin, marital status, and other demographic data	NO
D. Commercial information	Transaction information, purchase history, financial details, and payment information	YES
E. Biometric information	Fingerprints and voiceprints	NO
F. Internet or other similar network activity	Browsing history, search history, online behavior, interest data, and interactions with our and other websites, applications, systems, and advertisements	YES
G. Geolocation data	Device location	YES
H. Audio, electronic, sensory, or similar information	Images and audio, video or call recordings created in connection with our business activities	NO

I. Professional or employment-related information	Business contact details in order to provide you our Services at a business level or job title, work history, and professional qualifications if you apply for a job with us	NO
J. Education Information	Student records and directory information	NO
K. Inferences drawn from collected personal information	Inferences drawn from any of the collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	NO
L. Sensitive personal Information		NO

We may also collect other personal information outside of these categories through instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation in customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to your inquiries.

We will use and retain the collected personal information as needed to provide the Services or for:

- Category A - As long as the user has an account with us
- Category B - As long as the user has an account with us
- Category D - As long as the user has an account with us
- Category F - As long as the user has an account with us
- Category G - As long as the user has an account with us
- Category H - As long as the user has an account with us

Sources of personal information

Learn more about the sources of personal information we collect in "What information do we collect?"

How we use and share personal information

Learn more about how we use your personal information in the section, "How do we process your information?"

Everway

Will your information be shared with anyone else?

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Learn more about how we disclose personal information in the section, "When and with whom do we share your personal information?"

We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

We have not disclosed, sold, or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. We will not sell or share personal information in the future belonging to website visitors, users, and other consumers.

Your rights

You have rights under certain US state data protection laws. However, these rights are not absolute, and in certain cases, we may decline your request as permitted by law. These rights include:

- **Right to know** whether or not we are processing your personal data
- **Right to access** your personal data
- **Right to correct** inaccuracies in your personal data
- **Right to request** the deletion of your personal data
- **Right to obtain a copy** of the personal data you previously shared with us
- **Right to non-discrimination** for exercising your rights
- **Right to opt out** of the processing of your personal data if it is used for targeted advertising (or sharing as defined under California's privacy law), the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects ("profiling")

Depending upon the state where you live, you may also have the following rights:

- Right to access the categories of personal data being processed (as permitted by applicable law, including Minnesota's privacy law)
- Right to obtain a list of the categories of third parties to which we have disclosed personal data (as permitted by applicable law, including California's and Delaware's privacy law)
- Right to obtain a list of specific third parties to which we have disclosed personal data (as permitted by applicable law, including Minnesota's and Oregon's privacy law)
- Right to review, understand, question, and correct how personal data has been profiled (as permitted by applicable law, including Minnesota's privacy law)
- Right to limit use and disclosure of sensitive personal data (as permitted by applicable law, including California's privacy law)

- Right to opt out of the collection of sensitive data and personal data collected through the operation of a voice or facial recognition feature (as permitted by applicable law, including Florida's privacy law)

How to exercise your rights

To exercise these rights, you can contact us by visiting:

https://docs.google.com/forms/d/e/1FAIpQLSfOrIvBVaQo9BBg50t7j8XeDdLda8QQV_KJ14Pl22cnOa8rTg/viewform, by emailing us at dataprotection@texthelp.com, or by referring to the contact details at the bottom of this document.

We will honor your opt-out preferences if you enact the Global Privacy Control (GPC) opt-out signal on your browser.

Under certain US state data protection laws, you can designate an authorized agent to make a request on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with applicable laws.

Request verification

Upon receiving your request, we will need to verify your identity to determine you are the same person about whom we have the information in our system. We will only use personal information provided in your request to verify your identity or authority to make the request. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud-prevention purposes.

If you submit the request through an authorized agent, we may need to collect additional information to verify your identity before processing your request and the agent will need to provide a written and signed permission from you to submit such request on your behalf.

Appeals

Under certain US state data protection laws, if we decline to take action regarding your request, you may appeal our decision by emailing us at dataprotection@texthelp.com. We will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If your appeal is denied, you may submit a complaint to your state attorney general.

California "Shine The Light" Law

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third

parties for direct marketing purposes and the names and addresses of all third parties with which we shared

personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us by using the contact details provided in the section "How can you contact us about this notice?"

14. Do other regions have specific privacy rights?

In Short: *You may have additional rights based on the country you reside in.*

Australia

We collect and process your personal information under the obligations and conditions set by Australia's Privacy Act 1988 (Privacy Act).

This Privacy Notice satisfies the notice requirements defined in the Privacy Act, in particular: what personal information we collect from you, from which sources, for which purposes, and other recipients of your personal information.

If you do not wish to provide the personal information necessary to fulfill their applicable purpose, it may affect our ability to provide our services, in particular:

- offer you the products or services that you want
- respond to or help with your requests
- manage your account with us
- confirm your identity and protect your account

At any time, you have the right to request access to or correction of your personal information. You can make such a request by contacting us by using the contact details provided in the section "How can you review, update, or delete the data we collect from you?"

If you believe we are unlawfully processing your personal information, you have the right to submit a complaint about a breach of the Australian Privacy Principles to the Office of the Australian Information Commissioner.

15. Do we make updates to this notice?

In Short: *Yes, we will update this notice as necessary to stay compliant with relevant laws.*

We may update this Privacy Notice from time to time. The updated version will be indicated by an updated "Revised" date at the top of this Privacy Notice. If we make material changes to this Privacy Notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

Everway

16. How can you contact us about this notice?

If you have questions or comments about this notice, you may contact our Data Protection Officer (DPO) by email at dataprotection@texthelp.com, by phone at +44 (0)28 9442 8105, or contact us by post at:

Data Protection Officer
Everway
2401 Sawmill Pkwy Suite 10-11

Huron, OH 44839
United States

17. How can you review, update, or delete the data we collect from you?

Based on the applicable laws of your country or state of residence in the US, you may have the right to request access to the personal information we collect from you, details about how we have processed it, correct inaccuracies, or delete your personal information. You may also have the right to request we limit the use or disclosure of your personal information or withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. To request to review, update, or delete your personal information, please visit:

https://docs.google.com/forms/d/e/1FAIpQLSfOrIvBVaQo9BBg50t7j8XeDdLda8QQV_KJ14Pl22cnOa8rTg/viewform.