

DATA PRIVACY AGREEMENT for

Lancaster Central School District

This Data Privacy Agreement ("DPA") is by and between the **Lancaster Central School District** ("EA"), an Educational Agency, and Texthelp Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency (EA):** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means student personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family

Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable student information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract that commenced on July 7, 2022 ("Service Agreement"); Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in this DPA. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework.

5. Contractor's Employees and Subcontractors

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to this DPA where the subcontractor will receive or have access to PII are consistent with those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees.
- (e) Contractor must not disclose PII to any unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

6. Training

To the extent required by law, the contractor shall ensure that all its employees and subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

7. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII pursuant to the service agreement. Contractor will automatically delete all PII from its servers after a period of two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks. The EA may use the administrator portal to delete all PII at any time or may request assistance from Contractor to delete PII at any time. The confidentiality and data security

obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon deletion of PII from both active servers and backups.

8. Data Return and Destruction of Data

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period prescribed by this agreement, or as expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. The EA may use the administrator portal to delete PII at any time or may request assistance from Contractor to do so. If not deleted by the EA, Contractor will automatically delete all PII from its servers after a period of no more than two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks.
- (b) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.

9. Commercial or Marketing Use Prohibition

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose, except that teachers may receive email communications regarding product updates or professional development opportunities from which they may opt out at any time.

10. Encryption

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

11. Breach

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the Breach which includes the

date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Michele Ziegler,
Data Protection Officer/Director of Instructional Technology and Accountability
Lancaster Central School District
177 Central Avenue
Lancaster, NY 14086
mziegler@lancasterschools.org

12. Cooperation with Investigations

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA.

13. Notification to Individuals

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full actual cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to this DPA, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to this DPA, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for this DPA are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.



Contractor Name:	Texthelp Inc
Signature:	 <small>Doug Rosette (Sep 21, 2022 12:32 EDT)</small>
Printed Name:	Douglas Rosette
Title:	President
Email:	d.rosette@texthelp.com
Date:	9/21/2022
Lancaster Central School District Data Protection Officer – Michele Ziegler	
Date: 9/21/22	Signature:  <small>Michele Ziegler (Sep 21, 2022 12:36 EDT)</small>

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Lancaster Central School District is committed to protecting the privacy and security of student protected data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purpose.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices including, but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student protected data elements collected by New York State (<http://www.nysed.gov/data-privacy-security/student-data-inventory>) is available for public review or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student protected data or teacher or principal Annual Professional Performance Review data. Any such complaint must be submitted, in writing, to: Michele Ziegler, Director of Instructional Technology, 177 Central Avenue, Lancaster, New York 14086. Additionally, parents have the right to have complaints about possible breaches of student protected data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; the email address is "cpo@mail.nysed.gov". The State Education Department's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Lancaster Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., Family Educational Rights and Privacy Act; Education Law Section 2-d);
3. The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to protect the data privacy and mitigate security risks; and
6. Address how the data will be protected using encryption while in motion and at rest.


Contractor Name:	Texthelp Inc
Signature:	 <small>Doug Rosette (Sep 21, 2022 12:32 EDT)</small>
Printed Name:	Douglas Rosette
Title:	President
Email:	d.rosette@texthelp.com
Date:	9/21/2022

EXHIBIT B – Bill of Rights for Data Privacy and Security

Supplemental Information for Contracts That Utilize Personally Identifiable Information

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Description of the purpose(s) for which Contractor will receive/access PII	The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.
Type of PII that Contractor will receive/access	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date: July 7, 2022 Contract End Date: July 6, 2023, unless renewed by the parties without service disruption.
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer PII to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • <input checked="" type="checkbox"/> Securely delete and destroy PII.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify the Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

Contractor Name:	Texthelp Inc
Signature:	<u><i>Doug Rosette</i></u> Doug Rosette (Sep 21, 2022 12:32 EDT)
Printed Name:	Douglas Rosette
Title:	President
Email:	d.rosette@texthelp.com
Date:	9/21/2022

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. **For every contract, the Contractor must review the following list and provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State.**

CONTRACTORS ATTACHED PLAN SHALL INCLUDE THE FOLLOWING:

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.
7	Describe your secure destruction practices and how certification will be provided to the EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 https://www.nist.gov/cyberframework/new-framework



attach company privacy policy here



Privacy Policy for Texthelp Products

ISMS 1.18 : Issue 1 Rev 25 : Auth RG

At Texthelp, we are committed to safeguarding and preserving the privacy of our website visitors and product users. This Privacy Policy explains what happens to any personal data that you provide to us or that we collect from you while you use our software or visit our site.

Texthelp have signed the [Student Privacy Pledge](#), and implement [FERPA](#), [COPPA](#), and comply with the [California Consumer Privacy Act \(CCPA\)](#), the [Australian Privacy Act](#) and the General Data Protection Regulation (EU GDPR) compliant data policies. All data stored by Texthelp is stored according to our [Information Security Policy](#).

It is a requirement of using Texthelp products that end-users are made aware of this Privacy Policy. In a school/college type environment where acceptance/consent dialogs would be detrimental to the student's user experience these are not shown 'in program' and should be made available to the students or employees by the institution or organization using the product.



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

such as the currently selected voice, and any document annotations.

Your Google or Microsoft account and personal information

You are uniquely identified by your Google or Microsoft email address. This information is used to determine the status of your current license. No other Google or Microsoft profile information is collected. You have a right to request erasure of this data should you wish to, otherwise it will be deleted 2 years after the expiry of the current contract.

Students and Personally Identifiable Information

Where possible the only student information that we store is the student's Login ID. We need to store this so that we can store the user's preferences and data, and to confirm that they are a licensed user. You are uniquely identified by your login address. A de-identified version of this information is used to determine the status of your Texthelp Product current license. No other Google or Microsoft profile information is collected. We may keep this de-identified data indefinitely however this does not prevent your right of erasure of your information should you request it.

Verifiable Parental Consent



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

with Texthelp by a School District, School or Teacher, Texthelp accepts that consent is authorized by that institution in lieu of parental consent.

Additional Data Stored by Fluency Tutor for Google

Because Fluency Tutor has a teacher dashboard and displays class rosters, and individual student running records some additional information is stored. This is stored in compliance with our [Information Security Policy](#), encrypted in transit and at rest. The data which is stored is:

- The Teacher or Student first and second name
- The Teacher or Student email address
- Their Google Profile image (if the school policy permits access)
- Audio recordings of the student
- Their running record (WCPM and teachers comments)

Additional Data Stored by WriQ

Because WriQ has a teacher dashboard and displays class rosters, and individual student writing records some additional information is stored. This is stored in compliance with our [Information Security Policy](#), encrypted in transit and at rest. The data which is stored is:

- The Teacher or Student first and second name

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- Their writing scores record (WriQ scores, document metrics and teachers comments)
- An encoded string containing student writing and the types of errors in the document.

Additional Data Stored by EquatIO Mathspace

Because Mathspace has a teacher dashboard and displays class rosters, and individual student Math documents some additional information is stored. This is stored in compliance with our [Information Security Policy](#), encrypted in transit and at rest. The data which is stored is:

- The student first and second name
- The student email address
- Their Google Profile image (if the school policy permits access)
- Teacher feedback for Mathspace assignments (Assignment score and teachers comments)
- The students Mathspace documents

Additional Data Stored by ReachDeck/Browsealoud

By default, Browsealoud does not capture any end user information. However, administrators may log into the ReachDeck/Browsealoud portal to manage their subscription.



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

Additional Data Stored by ReachDeck Auditor

The Auditor feature does not process or store any personally identifiable information.

Additional Data Stored by ReachDeck Editor

Whilst the ReachDeck Editor does not request personal information, the purpose of the product is to help the User improve the readability of their content. Therefore the user will be entering information into this product. The information entered is sent to Texthelp for processing, however it is not stored and is deleted immediately after processing.

Additional Data Stored by OrbitNote

When using the OCR Scanning feature, PDFs that are sent for OCR are stored by Texthelp for 24 hours to ensure repeated requests are cached for optimum performance. After this period, the PDF is automatically deleted.



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

Required Permissions

Applications that integrate with a Microsoft, Chrome or a Google account must declare their intent by [requesting permissions](#). These permissions to your browser and account must be granted in order to integrate with your Microsoft, Chrome or Google accounts. Below is a list of these permissions and why they are required. At no time will Texthelp request or have access to your Microsoft or Google account password.

Read&Write for Windows, Mac, Google & Edge

Read&Write for Google Chrome Extension permissions

- Read and change all your data on all websites
 - Used by the reading and prediction features etc. to read and modify content.
- Know your email address
 - For licensing, storing settings
- Manage your apps, extensions and themes
 - Used to integrate with other Texthelp extensions such as WriQ.



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- We need your permission to open the PDF, KES and EPUB files from your Google Drive menus.
- **See, edit, create, and delete only the specific Google Drive files you use with this app**
 - We need your permission to open the PDF, KES and EPUB files from your Google Drive in our accessible viewers.
- **See, edit, create, and delete all of your Google Drive files**
 - Used to create the collected highlights, vocabulary and voice notes files.
- **See, create, and delete its own configuration data in your Google Drive**
 - Used to store the location of the voice notes folder
- **View your Google Drive apps**
 - Used to create the voice notes folder.

Google Drive Open with PDF and Epub viewers

- **View your email address**
 - For licensing, storing settings, and the annotations that you make on PDF and EPub Files.
- **View basic information about your account**
 - For licensing, storing settings, and annotations.

Screenshot Reader Extension

- **Read and change all your data on the websites that you visit**



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

Extension permissions

- Read your browsing history
 - Required to identify if we can display the toolbar.
- See your email address
 - For licensing and storing settings.
- Manage your apps, extensions and themes
 - Check if other Texthelp extensions are installed.
- Read and change content on websites you visit
 - Used by the reading and prediction features etc. to read and modify content.

Microsoft Account permissions

- Read your profile
 - For licensing and storing settings
- View your email address
 - For licensing and storing settings
- View your basic profile
 - For licensing and storing settings
- Sign you in
 - For licensing and storing settings

Google Documents integration

- View and manage your documents in Google Drive
 - We need permission to make a new Google Doc for you when we create the collected highlights and vocabulary documents.
- Connect to an external service
 - We need permission to connect to the Texthelp Vocabulary service. This service provides dictionary definitions, and symbols to be



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- View your Google Classroom classes
 - Used by DataDesk to display the list of your classes if logged in as a teacher.
- View your Google Classroom class rosters
 - Used to get a list of students for each class.
- View the email addresses of people in your classes
 - Used to toggle a student's features and to retrieve analytics.

Read&Write Admin Tool permissions

- View groups on your domain
 - Used to select Google groups to sync with Read&Write licensing.
- View users on your domain
 - Used to get the students within the selected groups to send to our licensing service. All user data is hashed before sending on. This encrypted hash cannot be decrypted by Texthelp or anybody else. We use the hashed value to identify users within Read&Write.

Read&Write Admin Tool Microsoft Account permissions

- Read your profile
 - For licensing and storing settings
- View your email address
 - For licensing and storing settings
- View your basic profile
 - For licensing and storing settings



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

OrbitNote

Google Drive Permissions

OrbitNote will only interact with the files you choose on your Google Drive. OrbitNote does not scan or interact with Google Drive files unless instructed to do so by the User.

- See and download all your Google Drive files
 - Used to open PDFs directly from Google Drive on a User's request.
- See, edit, create and delete all of your Google Drive files
 - Used to Upload PDFs to Google Drive on a User's request.
- View your Google Drive apps
 - Used to Check the required Texthelp Apps are installed.
- Manage your coursework and view your grades in Google Classroom
 - Used to check if a PDF is part of your active coursework within Google Classroom.
- View coursework and marks for students in the Google Classroom classes that you teach or administer
 - Used to check the status of PDFs within your Google Classroom classes.
- View your coursework and grades in Google Classroom
 - Used to check if a PDF is part of your active coursework



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- Manage your Google Classroom classes
 - Used to check if a PDF is part of your active coursework within Google Classroom.

Snapverter

Google Drive integration

- View your email address
 - For sending emails and displaying on dashboard..
- View basic profile info
 - For licensing and storing settings.
- View and manage Google Drive files opened or created with this app
 - We need your permission to open PDF, JPG, TIFF, GIF, PNG and ZIP (Daisy) files in your Google Drive.
- View and manage files in your Google Drive
 - We need your permission to open and add PDF, JPG, TIFF, GIF, PNG and ZIP (Daisy) files in your Google Drive.
- Have offline access
 - We need offline access to allow the conversion process to open and save files in your Google Drive.

Fluency Tutor for Google

Google Drive Permissions

- View your email address



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

install Fluency Tutor for Google as the default viewer for reading passages.

- **Have offline access**
 - We need offline access to allow the conversion process to open and save files in your Google Drive.

Android App permissions

- **View your email address**
 - For sending emails and displaying on dashboard..
- **View basic profile info**
 - For licensing and storing settings.

You can revoke these permissions at any time on your [Google Account Permissions](#) page.

EquatIO

EquatIO Chrome Extension Permissions

-
- **Read and change all your data on the websites you visit**
 - We read the browsing history so we can access the URL so we know which Google Apps integration to insert the math into.
 - This is required for us to drop the toolbar on top of Google Apps.
 - This is required for us to drop the floating toolbar onto any web page.
- **Know your email address**
 - Your email address is required for licensing.



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- View your basic profile info
 - Your email address is required for licensing

Google Apps Permissions

- View and manage your Google Docs documents
 - This may be required to insert math into the currently opened Google Doc
- View and manage your Google Slides presentations
 - This may be required to insert math into the currently opened Google Slide
- See, edit, create, and delete your spreadsheets in Google Drive
 - This is required for us to replace EquatIO Image URLs with images of math inside the currently opened Google Sheet
 - This may be required to insert math into the currently opened Google Sheet





Published using Google Docs

[Learn more](#)[Report Abuse](#)

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

on a number of websites

- Used to insert the WriQ sidebar into Google Docs and display the errors on the document.
- This allows WriQ to appear by default in Google Docs and Google Classroom and access the marking services.
 - All texthelp.com sites
 - classroom.google.com
 - docs.google.com
- Read your browsing history
 - Used to read the url of the current tab so WriQ can automatically be displayed
- Communicate with cooperating websites
 - Used to integrate with other Texthelp web applications
- Know your email address
 - For licensing, storing settings
- Manage your apps, extensions and themes
 - Used to integrate with other Texthelp extensions such as Read & Write.

Google Docs (Chrome extension only)

- View and manage your documents in Google Drive
 - This is required to score the document

Google Drive (Chrome extension only)



ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- **See and download all your Google Drive Files**
 - This is required to check you have access to the document you plan to score with WriQ and to retrieve the author of the document
- **View and manage its own configuration data in your drive**
 - This is required to store the configuration data and writing statistics

Google Classroom (WriQ Teacher Dashboard only)

- **View the email addresses of people in your classes**
 - This is required to import your students and classrooms from Google Classroom
- **View the profile photos of people in your classes**
 - This is required to import your students and classrooms from Google Classroom
- **View your Google Classroom class rosters**
 - This is required to import your students and classrooms from Google Classroom
- **View your Google Classroom classes**
 - This is required to import your students and classrooms from Google Classroom
- **Manage coursework and grades for students in the Google Classroom classes that you teach and view the coursework and grades for classes that you administer**
 - This is required to create and manage Google Classroom assignments through WriQ



Published using Google Docs

[Learn more](#)[Report Abuse](#)

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

- Your email address is required for licensing.
- **View your basic profile info**
 - Your email address is required for licensing.

WriQ for Microsoft Word (Word Addin and WriQ Dashboard)

Permissions Required

- **View users email address**
 - Your email address is required for licensing.
- **Read all files that user can access**
 - This is required to score the document and identify the author
- **Sign users in**
 - Your email address is required for licensing.
- **View users basic profile**
 - Your email address is required for licensing.
- **Read&Write access to users profile**

This is required to display the errors within a document

ReachDeck / Browsealoud

ReachDeck / Browsealoud Portal

- **View your email address**
 - Your email address is required for licensing

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

Express permission of the provider administrator or contact at the time of purchase for a site or group license. Similar express permission from a single user license owner or trialist must be provided.

Disclosing your information

We will not disclose your personal information to any other party other than in accordance with this Privacy Policy and in the circumstances detailed below:

- Where we are legally required by law to disclose your personal information.

Scraping Content

We do not scrape any personal content. Our systems are not designed to associate personal information with your activities.

We don't sell your personal data to other companies.

We never sell any personal information. Occasionally our products need to send your personal data (such as name, email,) to 3rd parties. These 3rd parties are our Hosting and Services providers. For Example, we use Amazon Web Services to host Fluency Tutor and WriQ. The database needs to store Student information so that we can display it for you and help you track progress. These data sharing partners do not disclose your personal information, and they store it with the same level of security or



Published using Google Docs

[Learn more](#)[Report Abuse](#)

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

through our software for ad targeting. We do not operate any referral program and do not display any sponsored links.

We take steps to protect personal information.

We take reasonable steps to secure your personally identifiable information against unauthorized access or disclosure. We encrypt transmission of data on pages where you provide payment information. However, no security or encryption method can be guaranteed to protect information from hackers or human error.

Information we collect may be stored or processed on computers located in any country where we do business.

Your rights to the personal information we may hold on you

You have the right to request the amending, erasure or a copy of your personal information that we may collect and store while you use our products. A Data Subject Access Request may be made [via this form](#). Alternatively you may telephone using the numbers on our '[Contact Us](#)' page or email to datasecurity@texthelp.com. We will respond to a request within these time limits.

United Kingdom 40 days, US 45 days, Canada 30 days, Australia 30 days.

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

stored in Amazon Web Services (AWS). We have entered into Standard Contractual Clauses with AWS to ensure we comply with the GDPR rules on international transfers. We have also included Standard Contractual Clauses in our End User License Agreement to cover the transfer of personal data from end users in the EU to AWS based in the United States. This complies with data protection requirements and GDPR legislation when transferring data outside of the EU.

Monitoring usage

Our software uses tracking software to monitor visitors to better understand how they use it. This is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website but will not store, save, or collect personal information. You can read Google's privacy policy [here](http://www.google.com/privacy.html) for further information <http://www.google.com/privacy.html>.



Google Analytics is a web analytics tool that helps website owners understand how visitors engage with their website. Google Analytics customers can view a variety of reports about how visitors interact with their website so they can improve it. Google Analytics collects information anonymously. It reports



Published using Google Docs

[Learn more](#)

[Report Abuse](#)

ISMS 1.18 Privacy Policy for Texthelp Products

Updated automatically every 5 minutes

Enforcement

We regularly review our compliance with our Privacy Policy. If we receive a formal written complaint, we will follow up and contact the person who made the complaint.

Changes

We do update this Policy from time to time, so please review this Policy regularly.