



Quote

Quote must be attached to Purchase Order
F.O.B Shipping Point

To: Boone County Schools

Address: 8330 US Highway 42
Florence, Kentucky 41042

ATTN: Randy Deaton

Date: May 28, 2020

Valid Until: August 11, 2020

Texthelp Inc.

500 Unicorn Park Dr. Floor 4
Woburn, MA 01801

Phone: 888-248-0652
Fax: 866-248-0652
Email: u.s.info@texthelp.com

Fed Tax ID# 06-1622277

Texthelp Contacts:

Marc Callahan
Rebecca McCarron
r.mccarron@texthelp.com

Quantity	Item	Type of License/Training	License Description:	Additional Information	Unit Price	Extended Price
20000	Read&Write	Unlimited	12 month renewable premium Unlimited (Domain-wide) Read&Write subscription for use by all students and staff within the school/district/specified domain, with take home access. Includes access to all supported platforms including Windows, Mac, Google Chrome, iPad and Android provided all technical requirements are met.	Subscription Aug 11, 2020 - Aug 11, 2021 Effective January 1, 2020, the retail list price for Read&Write is \$1.80 per student.	\$1.80	\$36,000.00
					Sub Total	\$36,000.00
					Sales Tax	\$0.00
					Total	\$36,000.00
<p>Note: Credit card payments will only be accepted for purchases of \$1000 or less, no credit card fees will be assessed. Note: A copy of the Tax Exempt ID Certificate must accompany order if applicable, otherwise sales tax may be charged.</p>						
<p>By using these products you are hereby agreeing to the terms of the relevant product End User License Agreements. These can be found at support.texthelp.com/help/end-user-license-agreements</p>						

Professional Development Offerings Available for Purchase:

Read&Write Onsite Training: 1 day (6 hours) Professional Development onsite at customer location. Hands-on for up to 25 participants. Can be delivered as two 3-hour workshops. Training resource materials provided. \$3000
Read&Write or EquatIO Training via Webinar: 2- or 3-hour Professional Development via webinar. Hands-on. Training resource materials provided. Includes copy of recorded webinar. \$500 (2hrs) \$600 (3 hrs)

Technical Support:

Online and telephone technical support is provided free of charge for duration of subscription.

Quotation Prepared by:

Rebecca McCarron

Texthelp Representative Signature:

Customer Representative Signature:

Confidential & Proprietary



Information Security Policy

ISMS 1.2 Information Security Policy : Issue 1 Rev 15 : Auth MMcK : Last reviewed 26-02-2020

Policy Summary

Texthelp will:

- Comply with both the law and best practice regarding information security and privacy
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff who handle personal data, so that they can act confidently and consistently

TexthelpLtd., Texthelp Inc. & Texthelp PTY recognizes that its first priority regarding information security and privacy is to avoid causing harm to individuals. Predominantly this means keeping information securely, on a need to know basis, in the right hands.

This is the top-level policy and, as well as outlining the company's information security objectives and how to meet them, it also includes a requirement for all security related documents to be reviewed periodically to ensure conformity and applicability.

It is the responsibility of all employees to comply with the requirements of this and all policies.

Objectives

Texthelp will:

- Deliver a secure, reliable cloud service for users and other interested parties who need confidence and assurance the platform is fit for their purpose of sharing and working with sensitive information.

- Provide a digital paperless ISMS for staff (and other interested parties who need to access it), integrated into their day to day work practices to ensure it becomes a habit for good performance not an inhibitor to getting their work done
- Implement a system to identify and assess information security risks and manage a risk treatment plan to mitigate risk to the confidentiality, integrity and availability of the information it holds or processes.
- Mitigate the risk of unauthorised or accidental disclosure of confidential information by staff or external parties
- Ensure the integrity and availability of the company's information assets at all times
- Minimize the impact of any security incidents
- Continually improve the company's ability to assess, detect, reduce, avoid and ameliorate information security risks and/or incidents
- Work to avoid a negative impact to Texthelp's reputation and brand
- Protect the information of all interested parties including the personal information of its customers.
- Comply with any legal, regulatory or contractual requirements in respect of the data it holds about individuals. These are listed in the [List of Legislative & Regulatory Bodies](#);
- Follow best practice
- Seek to continually improve the company's Information Security Management System

Key Risks & Mitigations

Texthelp has identified the following potential key risks, which this policy, in conjunction with the Risk Treatment Plan, is designed to address:

Risk	Mitigation
Breach of security by an external information asset	The development and implementation of information security Standards to minimize the risk of data being obtained by hacking or interception. Network security controls and physical perimeter security devices prevent the physical theft of the company's information assets by on-site contractors.
Release of data by a staff member	Staff Awareness Training will be delivered to help staff understand their responsibilities when handling personal data in order to prevent accidental disclosure of sensitive information. Access controls are in place to prevent unauthorised access to the company's information assets. Regular Audits will be conducted to ensure staff are complying with this policy
Exposure of sensitive information through hacking of Texthelp products or services	Secure development/coding practices will be employed and development staff training delivered. Testing of our products prior and after release will include, but not be limited to, the OWASP top-ten online vulnerabilities.

Not being able to respond to a security breach effectively	Texthelp will develop and manage an information security management system to maximize information security and manage security incidents. A Security Incident Response Policy exists outlining steps to be taken in the event of a security breach.
--	--

Responsibilities

information security Committee

The role and responsibilities of this committee will be to provide:

- Analysis & Design - The committee is also responsible for the analysis and design of the ISMS to ensure a meaningful security policy as well as effective security solutions exist.
- Administration - To look after the day to day administration of access rights, passwords, etc.
- Monitoring - To continuously monitor the security status of the organization, and manage incident response procedures.
- Awareness communication - To ensure awareness communication is conveyed throughout the company to ensure ongoing security awareness and also to provide the necessary training programs.
- Provide executive custody and governance - represented by the information security Committee.

Data Protection Officer

The Data Protection Officer is currently David Hankin who deals with both the day to day management of the Information Security Management System as well as continuous communication of the importance and value of security measures. with the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Specific other staff

IT & Network Administrator:

- Maintaining a secure network
- Maintaining access control lists to core services
- Implement and run the Business Continuity Plan and Disaster Recovery Plan
- Provide computing resources to deliver the Information Security Policy

Chief Data Officer:

- Manage and control access to Customer Data in the company CRM System
- Ensure that the customer data is stored in compliance with the information security Standards

Staff

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Enforcement

Significant breaches of this policy will be handled under Texthelp's disciplinary procedures.

Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, Texthelp has a separate Data [Privacy Policy](#).

Scope

This Policy applies to all employees and third-party agents of Texthelp as well as any other Company affiliate who is authorized to access customer Data. Third party agents of Texthelp will be required to have an Information Security Policy at least as stringent as this policy.

Third party agents will also be contractually required, where this is possible, to return or destroy information assets belonging to Texthelp upon termination of a contract with a third party. This will apply to both virtual and physical information assets.

Texthelp will comply with requests under the **Regulation of Investigatory Powers Act 2000 (RIPA)** from UK authorities and under the **USA Patriots Act** from US authorities and **Freedom of Information and Protection of Privacy Act (FOIPPA)(British Columbia)** and other agencies where obliged to do so if requested.

The full list of regulatory and legislative requirements with which Texthelp complies are given in this table of [Legislative & Regulatory bodies](#)

What we do with customer data

Texthelp has a [privacy policy](#) for Users, setting out how their information will be used.

Texthelp Staff Responsibilities

All Texthelp Staff are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix A)

Information Security Standards

All information that is stored by Texthelp is classified as one of the following data types:

- Public Information
- Company Intellectual Property

- Customer/Personal Information
- (other) Confidential Information

All data that is classified as ‘Customer Information’ or ‘Company IP’ must be stored in compliance with the following standards.

- Encrypted at Rest
- Encrypted in Transit using SSL Encryption
- All Access to the information is Logged
- Access protected by two factor authentication
- All data must be stored in an ISO 27001 or equally secure facility
- All data must be backed up regularly and securely
- Information assets should be recorded in the company’s Asset Register
- Any relevant information security contracts that have been entered into between Texthelp and a Customer must be recorded in the Information Security Management System

Physical Media Transfer : no customer or private data will be transported using physical media
In order to comply with relevant legislation:

- If Texthelp is storing information relating to or created by a student (Student Data), that data should be deleted if a request to do so is made by a parent of the student. If appropriate Texthelp will ask the Parent, School or District to verify that the request is valid.
- Texthelp has a policy not to retain Student Data once 180 days after a subscription has lapsed. In the case of the Fluency Tutor product any data that is stored is only stored to deliver the functionality of the product for the district and is strictly for Education Purposes. Upon request Texthelp will delete any Student Data immediately.
- Texthelp will store customer, student, supplier and job applicant data for a minimum of 6 years. Any student data that is stored is only stored to deliver the functionality of the product. Upon request Texthelp will delete any customer, student or job applicant data thereby complying with the GDPR’s Right to Erasure requirement.

Texthelp must operate a Business Continuity Plan to deliver continuity of service in the event of a disaster. This plan should cover situations such as:

- Fire
- Flash flood
- Pandemic
- Power Outage
- Theft

Information Security Management System

A system must be maintained to manage and control the security of all data stored by Texthelp. The system must:

- List all information assets including:
 - Their Physical Location
 - Their Data Classification based on the:

- Value
 - Criticality
 - Sensitivity
- The method of encryption for storage at rest
 - The method of encryption for data in transit
 - Whether the information asset contains user data
 - Who can access the data
- List all data contracts including:
 - What products the customer is using
 - What information asset their data is stored in
 - Who to notify in the event of a security breach
- Manage Security Incidents including:
 - Provide a means of notifying all relevant customers and staff
 - Record all security incidents
 - Resolve the security incident and record steps taken to prevent recurrence
- Where relevant, record access to information assets by staff members including
 - Which staff member
 - Which data
 - What date and time

Staff training & acceptance of responsibilities

Documentation

Information for staff and temporary workers is contained in the staff handbook.

Induction

All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.

Data Protection will be included in foundation training for all staff.

Continuing training

Texthelp will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Procedure for staff signifying acceptance of policy

All staff are required to sign an electronic form signifying that they have read, understood and accept this policy.

Specific Focus Training for Key Handling Roles

Software Developers

Software Developers at Texthelp will be trained to ensure that the architecture of any system that stores personal data is in compliance with the information security Standards above. Prior to release the software will be tested to ensure that it is in compliance. All Product Owners, Scrum-masters or Project leaders should ensure that an Information Security Risk Assessment is carried out for each sprint, and when needed, a risk treatment plan is created and followed.

Marketing Staff

Marketing Staff who have access to personal customer information will receive specific training regarding the secure transit and storage of personal data for the purposes of outbound marketing.

Policy review

Responsibility

David Hankin (Quality Manager) will be responsible for reviewing this policy. This Information Security Policy will be audited as a part of the company's scheduled ISO 27001 audits. Audits of all processes within the company will take into account this Information Security Policy at all times.

Procedure

An annual review of the policy will be performed to ensure continuing relevance. The results of this review will be available on request.

Timing

An audit of this policy will be carried out once per year. However, the requirements of this policy, with regard to data privacy/security, will form a part of the company's regular ISO 9001 internal audits. The ISO 9001:2015 audits are performed twice annually.

information security Incidents

All information security incidents will be logged in the [Downtime/Security Events Register](#) in Sugar. Information security incidents will be classified according to severity. Incidents such as unsuccessful exploit attempts that do not involve data loss will be classified as Level 1 - Non Critical Incidents. Level 1 incidents should not trigger a customer notification since there has been no impact to privacy. Incidents that do involve data loss will be classified as Level 2 - Critical Incidents & should trigger a notification to all customers that are impacted by the data loss. The Information Commissioner's Office should also be notified within 72 hours of the breach being discovered.

Appendix A: Confidentiality statement for staff

When working for Texthelp , you will often need to have access to confidential information which may include, for example:

Personal information about individuals who are customers or users of Texthelp software.

Information about the internal business of Texthelp.

Personal information about colleagues working for Texthelp.

Texthelp is committed to keeping this information confidential, in order to protect people and Texthelp. 'Confidential' means that all access to information must be on a need to know and properly authorized basis. You must use only the information you have been authorized to use, and for purposes that have been authorized. You should also be aware that under the Data Protection Act, unauthorized access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Texthelp to be made public. Passing information between staff members in our international office, or between Texthelp and a 3rd party marketing partner who is in compliance with our policy, or vice versa does not count as making it public, but passing information to another organization does count.

You must also be particularly careful not to disclose confidential information to unauthorized people or cause a breach of security. In particular you must:

not compromise or seek to evade security measures (including computer passwords);


be particularly careful when sending information between our international offices;

not discuss confidential information, either with colleagues or people outside Texthelp;

not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorized to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Texthelp .

Signed:  (CEO)



Signed:

(CTO)

Public Information