Rosetta Stone Ltd.
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

March 1, 2019 To February 29, 2020

Table of Contents

SECTION 1

ASSERTION OF ROSETTA STONE LTD. MANAGEMENT

ASSERTION OF ROSETTA STONE LTD. MANAGEMENT

March 5, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Rosetta Stone Ltd.'s ('Rosetta Stone' or 'the Company') Rosetta Stone SaaS and Lexia Learning SaaS Services System throughout the period March 1, 2019 To February 29, 2020, to provide reasonable assurance that Rosetta Stone's service commitments and system requirements relevant to Security, Confidentiality, and Privacy (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Rosetta Stone Ltd.'s Description of Its Rosetta Stone SaaS and Lexia Learning SaaS Services System Throughout the Period March 1, 2019 To February 29, 2020" and identifies the aspects of the system covered by our assertion.

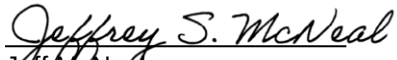
We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2019 To February 29, 2020, to provide reasonable assurance that Rosetta Stone's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and Rosetta Stone's compliance with the commitments in its privacy notice throughout the period March 1, 2019 To February 29, 2020. Rosetta Stone's objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Rosetta Stone Ltd.'s Description of Its Rosetta Stone SaaS and Lexia Learning SaaS Services System Throughout the Period March 1, 2019 To February 29, 2020".

Rosetta Stone uses Amazon Web Services ('AWS') to provide cloud hosting services, Google Cloud Platform Services ('GCPS') to provide cloud hosting services, Microsoft Azure ('Azure') to provide cloud hosting services, and Evoque Data Center Solutions ('Evoque') to provide colocation services (collectively, 'subservice organizations'). The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Rosetta Stone, to achieve Rosetta Stone's service commitments and system requirements based on the applicable trust services criteria and Rosetta Stone's compliance with the commitments in its privacy notice. The description presents Rosetta Stone's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Rosetta Stone's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Rosetta Stone's service commitments and system requirements based on the applicable trust services criteria and Rosetta Stone's compliance with the commitments in its privacy notice. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Rosetta Stone's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 1, 2019 To February 29, 2020 to provide reasonable assurance that Rosetta Stone's service commitments and system requirements were achieved based on the applicable trust services criteria.



Jeff McNeal
Director of Datacenter and Enterprise Services
Rosetta Stone Ltd.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Rosetta Stone Ltd.:

Subject

We have examined Rosetta Stone Ltd.'s ('Rosetta Stone' or 'the Company') accompanying description of Rosetta Stone SaaS and Lexia Learning SaaS Services System titled "Rosetta Stone Ltd.'s Description of Its Rosetta Stone SaaS and Lexia Learning SaaS Services System Throughout the Period March 1, 2019 To February 29, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2019 To February 29, 2020, to provide reasonable assurance that Rosetta Stone's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and Rosetta Stone's compliance with the commitments in its privacy notice throughout the period March 1, 2019 To February 29, 2020.

Rosetta Stone uses Amazon Web Services ('AWS') to provide cloud hosting services, Google Cloud Platform Services ('GCPS') to provide cloud hosting services, Microsoft Azure ('Azure') to provide cloud hosting services, and Evoque Data Center Solutions ('Evoque') to provide colocation services (collectively, 'subservice organizations'). The description indicates that complementary subservice organizations controls that are suitably designed and operating effectively are necessary, along with controls at Rosetta Stone, to achieve Rosetta Stone's service commitments and system requirements based on the applicable trust services criteria and Rosetta Stone's compliance with the commitments in its privacy notice. The description presents Rosetta Stone's controls, the applicable trust services criteria, and the types of complementary subservice organizations controls assumed in the design of Rosetta Stone's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organizations controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Rosetta Stone, to achieve Rosetta Stone's service commitments and system requirements based on the applicable trust services criteria and Rosetta Stone's compliance with the commitments in its privacy notice. The description presents Rosetta Stone's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Rosetta Stone's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Rosetta Stone is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Rosetta Stone's service commitments and system requirements were achieved. Rosetta Stone has provided the accompanying assertion titled "Assertion of Rosetta Stone Ltd. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Rosetta Stone is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements and complying with the commitments in its privacy notice.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and its compliance with the commitments in its privacy notice. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and its compliance with the commitments in its privacy notice
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria and its compliance with the commitments in its privacy notice
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Rosetta Stone's Rosetta Stone SaaS and Lexia Learning SaaS Services System were suitably designed and operating effectively throughout the period March 1, 2019 To February 29, 2020, to provide reasonable assurance that Rosetta Stone's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Rosetta Stone's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Rosetta Stone, user entities of Rosetta Stone's Rosetta Stone SaaS and Lexia Learning SaaS Services during some or all of the period March 1, 2019 To February 29, 2020, business partners of Rosetta Stone subject to risks arising from interactions with the Rosetta Stone SaaS and Lexia Learning SaaS Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organizations controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

March 5, 2020
Tampa, Florida

SECTION 3

ROSETTA STONE LTD.'S DESCRIPTON OF ITS ROSETTA STONE SAAS AND LEXIA LEARNING SAAS SERVICES SYSTEM THROUGHOUT THE PERIOD MARCH 1, 2019 TO FEBRUARY 29, 2020

OVERVIEW OF OPERATIONS

Company Background

Rosetta Stone Ltd. (“Rosetta Stone”) is dedicated to changing people's lives through the power of language and literacy education. The Company’s innovative digital solutions drive positive learning outcomes for the inspired learner at home or in schools and workplaces around the world.

Founded in 1992, Rosetta Stone uses cloud-based solutions to help all types of learners read, write, and speak more than 30 languages. Lexia Learning Systems LLC (“Lexia”), a wholly owned subsidiary of Rosetta Stone and Rosetta Stone's literacy education division, was founded more than 30 years ago and is a leader in the literacy education space. Today, Lexia helps students build foundational reading skills through its rigorously researched, independently evaluated, and widely respected instruction and assessment programs. Lexia was formed as a limited liability company in Delaware in 2013. Rosetta Stone was incorporated in Virginia in 1992.

Rosetta Stone continues to emphasize the development of technology-based products and services for Corporate, Government and K-12 learners who seek best-in-class solutions to achieve their literacy, assessment, and language-learning objectives. This focus extends to the Consumer Language segment, where the Company continues to make product investments serving the needs of passionate language-learners who are mobile, results-focused and value a quality language-learning experience.

Description of Services Provided

Rosetta Stone’s business is organized into three operating segments: Literacy, Enterprise and Education (E&E) Language, and Consumer Language. The Literacy segment derives revenue under a SaaS model from the sales of language, literacy and literacy assessment solutions to educational institutions serving grades K through 12. The E&E Language segment derives revenues from sales of Rosetta Stone enterprise language-learning solutions to educational institutions, corporations, and government agencies worldwide under a SaaS model. The Consumer Language segment derives revenue from sales of personal use language-learning offerings to individuals directly and through retail partners worldwide, and has completed its migration to SaaS from a packaged software business. Many of the Literacy, E&E Language, and Consumer Language products and services are supported and accessible as mobile apps for tablets and smartphones enabling learners to continue their lessons on the go and extend the learning experience away from a desk-top computer. Progress is automatically synchronized across devices to meet the customers' and learners’ lifestyles.

Products and Services

Literacy

Literacy Solutions: Rosetta Stone’s Literacy segment is comprised solely of the Lexia business. The Lexia suite of subscription-based literacy learning and assessment solutions provide explicit, systematic, personalized learning on foundational literacy skills for students of all abilities. This research-proven, technology-based approach accelerates reading skills development, predicts students' year-end performance, and provides teachers with data-driven action plans to help differentiate instruction. The Lexia Core5 Reading® program is available for all abilities from pre-K through grade 5. The Lexia® PowerUp Literacy™ program is designed for non-proficient readers in grades 6 and above. The Lexia® RAPID® Assessment solution is a computer-adaptive screener and diagnostic tool for grades K-12 that identifies and monitors reading and language skills to provide actionable data for instructional planning. All of the Lexia solutions deliver performance data and analysis to enable teachers to monitor and modify their instruction to address specific student needs. These literacy solutions are provided to schools as web- and mobile app-based site-wide or multi-seat subscription licenses. Rosetta Stone’s service offerings provide schools with product implementation services to support strong educator and student use. Lexia subscriptions and services are purchased through annual or multi-year service contracts.

E&E Language

E&E Language-Learning Solutions: Rosetta Stone provides a series of web- and mobile app-based subscriptions to interactive language-learning solutions for schools, businesses, government agencies, and other enterprise organizations. The core language-learning suite offers courses and practice applications in multiple languages, each leveraging Rosetta Stone's proprietary context-based immersion methodology, speech recognition engine and innovative technology features. Available in 24 languages and designed for beginner to intermediate language learners, the Rosetta Stone® Foundations™ program builds fundamental language skills. The Rosetta Stone® Advantage™ program is available for all proficiency levels in 9 of the 24 languages and focuses on improving every-day and business language skills. The Rosetta Stone® Advanced English for Business™ solution was designed to serve multinational companies seeking to build their employees' English language proficiency to support their ability to communicate and operate in a global business environment. In 2016, Rosetta Stone completed the development of the Rosetta Stone® Catalyst™ solution, which consolidates and aligns the *Foundations*, *Advantage* and *Advanced English for Business* products into a single solution for enterprise customers. Catalyst provides streamlined access and simplified pricing for the full suite of English and world language learning content, along with assessment, placement, ongoing reporting and demonstration of results, all of which more fully address important customer needs to focus and demonstrate efficacy and support progress across a range of learner skill levels. Specifically designed for use with these language-learning solutions, E&E Language customers with active subscriptions may also purchase companion audio practice products, as well as live tutoring sessions, to enhance the learning experience. Rosetta Stone offers tailoring of its solutions to help its enterprise customer organizations maximize the success of their learning programs. Current custom solutions include curriculum development, global collaboration programs that combine language education with business culture training, group and live tutoring, and language courses for mission-critical government programs.

Rosetta Stone's Literacy and E&E Language solutions include administrative tools, as well as options for professional services and support.

Enterprise Administrator Access and Administrative Tools: The Literacy and E&E Language programs include client administrator-level access, with a set of administrative tools that enable the client administrator to manage learner access, monitor performance, and measure and track learner progress. Administrators can also use these tools to access real-time dynamic reports, to identify each learner's strengths and weaknesses, and to inform instructional plans.

Professional Services: Professional services provide the enterprise customers with access to the experienced training, implementation and support resources. The training, implementation and support teams work directly with customers to plan, deploy, and promote the program for each organization, incorporate learning goals into implementation models, prepare and motivate learners, and integrate the Literacy and/or E&E Language solutions into the technical infrastructure. Some of the Literacy and E&E Language solutions include the option for additional online services to enhance and augment the learners' capabilities. For the E&E Languages solutions, Online Tutoring is an online video-interactive service, available to enterprise customers with active subscriptions, that provides either one-on-one or group conversational coaching sessions, led by native speakers, to practice skills and experience direct interactive dialogue.

Consumer Language

Rosetta Stone offers a broad portfolio of technology-based learning products for personal use to the global consumer. The portfolio of interactive language-learning solutions is powered by the widely recognized brand and built upon Rosetta Stone's 25+-year heritage in language-learning. Rosetta Stone Consumer Language-Learning Solutions: Rosetta Stone provides intuitive, easy-to-use, language-learning programs that can be purchased primarily as Software as a Service subscriptions via the web, mobile in-app purchase, or through retail channels.

The language-learning suite offers courses and practice applications in multiple languages, each leveraging the proprietary immersion methodology, speech recognition engine and innovative technology features. Beginner language-learning products are available in multiple languages to build fundamental language skills. Rosetta Stone also offers its consumer customers online services to enhance and augment the learners' capabilities. Online Tutoring is an online video-interactive service available to consumer customers with active subscriptions, that provides either one-on-one or group conversational coaching sessions, led by native speakers, to practice skills and experience direct interactive dialogue. Rosetta Stone Consumer solutions are supported and accessible as both web-based and mobile apps for tablets and smartphones, enabling learners to continue their lessons on the go and extend the learning experience away from the desk-top computer. Progress is automatically synchronized across devices to meet the Company's learners' lifestyles.

Principal Service Commitments and System Requirements

Rosetta Stone designs its processes and procedures for its Literacy, E&E Language, and Consumer solutions to meet its objectives. Those objectives are based on the service commitments that the Company makes to its educational and enterprise clients, consumer customers, and end users/learners; the laws and regulations that govern the provision of the products and services it offers and supports; and the financial, operational, and compliance requirements that the Company has established for its products and services. The products and services that the Company offers, and the associated data processing activities, are subject to a number of data privacy and security laws and regulations based on the jurisdictions in which the Company operates and the industry sectors Rosetta Stone serve and support, including, but not limited to, the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, the EU General Data Protection Regulation (GDPR), the Family Educational Rights and Privacy Act (FERPA), and other federal and state data privacy and security laws and regulations.

Security commitments to customers and users are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Given the multi-tenant, shared database SaaS architecture of Rosetta Stone's solutions, security commitments are standardized within channels and/or product lines.

Security principles within the fundamental designs of the Company SaaS applications and the Company systems and internal infrastructure environments used to support the SaaS applications, are designed to permit Company system users to access the information they need based on their role in the system and Company organization, while restricting access to information not needed for their role.

Company solutions utilize encryption technologies to protect customer data both at rest and in transit. The Company maintains administrative, technical and operational requirements designed to support the achievement of security commitments, legal and regulatory compliance obligations, and other system requirements, while serving the needs of the customers and learners. Such requirements are reflected and communicated in Rosetta Stone's system policies and procedures, system design documentation, internal awareness and training, and in the contracts with the customers. Information security policies are designed to reflect an approach to protecting data and systems that is both multi-layered and organization wide. These include policies around how new products and services are designed, developed, and maintained (including Privacy & Security by Design principles); how the associated systems are operated; how internal business systems and networks are managed; and how employees are hired and trained. In addition to the policies, standard operating procedures documenting how to carry out specific manual and automated processes required in the operation and development of the Company SaaS products and services are utilized.

Components of the System

Infrastructure

Primary infrastructure used to provide Rosetta Stone's Rosetta Stone SaaS and Lexia Learning SaaS Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
VMware EX Servers	Lenovo, HP	Private cloud environment
Physical Linux Servers	HP	Private cloud environment
AWS Virtual Servers	EC2	Public Cloud Product delivery
Kubernetes Cluster	Lenovo	Container delivery
Firewalls	Cisco Adaptive Security Appliances (ASA)	Perimeter Firewall, Virtual Private Network (VPN), Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
Switches	Cisco	Core switching
Storage Arrays	Nimble	Storage Area Network (SAN) storage arrays
Routers	Cisco	Router
Load Balancer & Web Application Firewall	NetScaler	Forward load balancing

Software

Primary software used to provide Rosetta Stone's Rosetta Stone SaaS and Lexia Learning SaaS Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VMware	VMware	Hypervisor
Microsoft Windows	Windows Servers 2008 R2	Active Directory
MySQL	Linux	Production database
In-House Developed software	Linux (Ruby, HyperText Pre-processor (PHP), Java, etc.)	Product delivery
Redis	Linux	Database
MongoDB	Linux	Database
Percona MySQL	Linux	Database
Aurora MySQL	Linux	Database
Elasticsearch	Linux	Search Data
Nginx, Apache	Linux	Web services

Primary Software		
Software	**Operating System**	**Purpose**
Actifio, Networker	N/A	Backups
Nagios, Prometheus, Splunk	Linux	Monitoring
Chef	Linux	Configuration management
Kubernetes	Linux	Production applications
Jenkins & Bamboo	Linux	Continuous integration/delivery
Stash, SVN	Linux	Source repository

People

The Company has a staff of approximately 1150 employees organized in the following functional areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, and human resources
- Operations. Research, marketing, sales, and staff that administers support services to customers and/or learners, including both contracted support services under services agreements, and direct support to learners as needed
- IT Help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom
    - The help desk group provides technical assistance to Company employees
    - The infrastructure, networking, and systems administration staff typically has limited direct day-to-day involvement in direct operations and support activities relating to customer and learner use of Company products and services, but rather serves to support and maintain the Company's IT infrastructure, which supports the systems and functionality comprising the SaaS software and services. A systems administrator manages deployment of releases of the SaaS products and other software and updates into the production environment in accordance with Company policies and protocols
    - The product & software development staff develops and maintains the core custom Company software for the Company solutions. This includes the product/application, supporting utilities, updates and patch management, and the external websites that interact with the product. The staff includes software developers, database administration, software quality assurance, and technical writers
    - The information security staff supports the Company product offerings indirectly by maintaining the Company infrastructure, networking, and systems administration, as well as monitoring internal and external security threats and maintaining current antivirus software
    - The information security staff maintains the inventory of IT assets
    - The IT operations staff manages the user interfaces for the Company solutions. This includes processing user entity-supplied membership and eligibility files, producing encounter claims files, and other user-oriented data (capitation files, error reports, remittance advice, etc.)
    - The Telecom staff maintains the Company voice communications environment, provides user support to the Company, and resolves Company communication problems. This group does not directly perform or support fulfillment of the Company SaaS solutions to customers and learners, but rather supports the Company infrastructure, as well as supporting disaster recovery assistance

Data

Under Company policies, Data associated with Company products and services, includes:

- Customer data
- Payment data
- Application data
- System & Diagnostic data

Customer Data

Customer data is received by the Company from customers and/or learners through the service agreements with enterprise customers, from individual consumers that purchase and/or use Company Consumer solutions, and through the sales, support and product development staff who assist customers and users.

Payment Data

Payment data is received by the Company from customers and/or consumers through the service agreements and through purchase of Company Consumer solutions, and through sales and support staff who assist customers and users.

Application Data

Application data is loaded into Company datastores (e.g., MySQL) during software releases or through content editors, or may be externally hosted by contracted service providers.

Examples of Application Data:

1. "Path Steps", which is non-PII data, about how a user has progressed through the product (would need to be coupled with PII data to "resolve" a support request for a particular customer/user).
2. Program content that defines the overall structure of how clients navigate Rosetta Stone's different language and literacy products (levels, activities, units, etc.).
3. Content assets incorporated into the product, such as images, text excerpts, audio samples, movies, etc.
4. Software control data.

System & Diagnostics Data

The Company utilizes various logs for both diagnostics and security. Types include:

1. Log data that originates from system logs, like Linux syslog. Much of this log data stays local to the machine that generates the log, but non-standard or suspicious activity would be identified and forwarded to internal issue monitoring or ticketing systems for easier searching, including for further internal review and potential issue escalation.
2. Application logs that are generated are forwarded to internal issue monitoring or ticketing systems. These are typically used by developers to diagnose and understand product operational data for improvement and optimization, since product developers do not have access to production data and logs directly.
3. Other diagnostics data includes programing back traces, which go to a specialized service for examination, and customer-side error reports ("crash reporting") that flow into analysis services.

Privacy Commitments

The following table describes the information included as part of the Rosetta Stone SaaS and Lexia Learning SaaS Services System of Rosetta Stone:

Client Data	Reporting
Rosetta Stone SaaS • First and Last Name • Address • Credit Card Number • E-mail Address • Telephone Number Lexia Learning SaaS • First and Last Name • Username • Grade • School • Instructional Language(English or Spanish)	Private data is recorded in Rosetta's internal databases to log personal information, usage activity, and current licensing information. This information is monitoring via database and server layer logging controls and is restricted to individuals with authorized access.

Rosetta Stone captures personal information when data subjects access and use the SaaS Services System. The types of personal information collected include name, address, e-mail address, telephone number, Internet Protocol (IP) address, web browser software, web referring service, and cookies. Users are required to provide basic personal information in order to use the service when registering.

Rosetta Stone's legal department is responsible for identifying specific requirements in agreements with user entities and in laws and regulations applicable to the personal information collected via the SaaS Services System. The legal department coordinates with the IT department and the privacy officer to implement controls and practices to meet those requirements.

ROSETTA STONE ONLINE INTERACTIVE PRODUCT PRIVACY POLICY

This Online Interactive Product Policy (the "Policy") explains Rosetta Stone's data collection, use, and disclosure practices for Rosetta Stone interactive online products and services, including without limitation the websites, software, hosted services, mobile and internet applications, trials and demos, content, games, audio and video, and associated documentation (each a "Service") owned and operated by Rosetta Stone Ltd. and/or any of its subsidiaries and affiliates. By accessing or using any Service, the customers signify that the customers have read, understand, and accept the terms of this Policy. If the customers are receiving access to a Rosetta Stone Service from or through an educational institution, government agency or business enterprise that is a party to a Rosetta Stone Enterprise License or similar agreement, and the terms of that Enterprise License Agreement conflict with the terms of this Policy, the terms of the Enterprise License Agreement will prevail with respect to the conflicting term(s). As used in this Policy, the term "Service" refers to the specific Service that the customers are accessing or using.

Rosetta Stone is committed to the privacy and security of personal information the employees receive and process, and for appropriately and promptly addressing requests and instructions regarding personal data, in accordance with applicable legal requirements. In order to better ensure the proper handling of data requests, the Company created a Personal Information Request web form to enable Rosetta Stone to support requests from individuals seeking information and action with respect to personal data the Company collected for those individuals and how the Company uses that information. If the customers are contacting Rosetta Stone to request information or action with respect to personal data the Company has collected about the customers, or to exercise their data protection rights, the Company asks that the clients please click HERE and submit their requests through the Personal Information Request web form.

If the customers have other specific questions about this Policy, please contact Rosetta Stone by e-mail at privacyofficer@rosettastone.com.

Information Collected

We receive and store any information the customers enter through the Service or give Rosetta Stone in any other way. This includes information that can identify the customers ("personal information"), including their first and last name, telephone number, postal and e-mail addresses. Rosetta Stone also may ask the customers to provide additional information about themselves, including their age, hobbies, and interests in learning languages. The customers can choose not to provide this additional information to us, but in general, some information about the customers is required in order for the customers to subscribe to or register and participate in the features offered through the Service.

Other than their personal information as described above, Rosetta Stone reserves the right to record, read, copy, disclose, and otherwise use any text, speech, data, images, and other materials that the customers transmit orally or by text or post to or through the Service or any of its components.

We automatically collect some information about their computer when the customers visit the Service. For example, Rosetta Stone will collect the IP address, Web browser software (such as Mozilla Firefox, Google Chrome, or Internet Explorer), and the referring web Service. Rosetta Stone also may collect information about their activity on this Service, such as the classes, games or chat rooms in which the customers participate. One of Rosetta Stone's goals in collecting this automatic information is to help improve their user experience. Finally, when the customers visit the Service, Rosetta Stone may assign their computer a "cookie" (a small, unique identifier text file) to remember who the customers are. For example, if the customers register on the Service, Rosetta Stone may record their password in a cookie for verification purposes. Rosetta Stone also may include other information in Rosetta Stone's cookie files; for example, if the client arrived at the Service via a link from third-party site, Rosetta Stone may include the URL of the linking page.

Please note that, unless the Service makes specific references to children and collects age information, the Service is not available for children under 13 years old in the United States or under another age specific to certain other countries in those locations. Accordingly, Rosetta Stone will not knowingly collect or maintain personal information from children under the required minimum ages through a Service that is not intended for children. Please see below for more information on Rosetta Stone's policies regarding children's privacy. If the client believes that Rosetta Stone might have any information from or about a child below the minimum age, please contact Rosetta Stone at privacyofficer@rosettastone.com.

Use of Personal Information

We will use personal information about the customers for the following general purposes: to process their subscription or registration to the Service; to provide the customers with the products and services the customer's request; to tailor their learning experience; to respond to their questions and comments; to communicate with the customers via regular mail and e-mail (or other electronic means) about Rosetta Stone's programs and services; to measure interest in and improve Rosetta Stone's offerings; to solicit information from you, including through surveys; to resolve disputes, collect fees, or troubleshoot problems; to prevent potentially illegal activities; to enforce Rosetta Stone's Terms of Use; and otherwise as described to the customers at the point of collection.

Please review "Their choices with respect to the Collection and Use of Personal Information" below.

Disclosure of Personal Information

We may display their profile information (minus their e-mail address and password) to other community members of the Service and to support other Service functions. Rosetta Stone also may disclose their personal information as follows:

(a) For processing orders, registrations and inquiries related to the Service.

(b) To third-party vendors who provide services or functions on Rosetta Stone's behalf, including customer service, business analytics, marketing, and services to Rosetta Stone in connection with operating the Service. These companies have access to information needed to perform their functions and are not permitted to share or use the information for any other purpose.
(c) To business partners with whom Rosetta Stone may jointly offer a product or service offering. The customers can tell when a third-party is involved because the third-party's name will appear on informational materials. If the customers choose to take advantage of these offerings, Rosetta Stone may share information about you, including personal information, with those named partners. Please note that the Company does not control the privacy practices of these third-party business partners.
(d) When advisable or necessary to conform to legal and regulatory requirements.
(e) As necessary, in Rosetta Stone's sole discretion, to protect the perceived rights, safety and property of Rosetta Stone, the Service's hosts and carriers, users of the Service, and the public.
(f) As necessary for resolving disputes, collecting fees, and troubleshooting problems.
(g) In connection with a change of control or operations, including without limitation in any merger, acquisition, reorganization, restructuring or any other transfer of Rosetta Stone's assets, or a transfer of the Service operations.
(h) Otherwise with their consent.
(i) To the educational institution, government agency or business enterprise through which the customers are receiving access to the Service when their access is granted through an Enterprise License or similar agreement between Rosetta Stone and such entity.
(j) To Rosetta Stone's instructors, to tailor their instructional materials and interactions with you.

Other than as set out above, the customers will be notified when personal information about the customers will be shared with third parties, and the customers will have an opportunity to choose not to have Rosetta Stone share such information.

Rosetta Stone also may share aggregate or anonymous information with third parties, including advertisers and investors. For example, Rosetta Stone may tell Rosetta Stone's advertisers the number of visitors to the Service. This information does not contain any personal information and is most often used to develop content and services that Rosetta Stone hope the customers find of interest.

A Special Word about Chat Rooms and E-mail

Please keep in mind that whenever the customers voluntarily disclose personal information online, that information can be collected and used by others. By posting personal information online or disclosing such information in 'voice chats' with other when using the Service, that information can be seen, collected and used by others besides us. Rosetta Stone cannot be responsible for any unauthorized third-party use of such publicly-accessible information.

Access to Personal Information

The customers may obtain a copy of any personal information about the customers that the customers provide through the Services or otherwise request that Rosetta Stone update or make changes to such personal information by using Rosetta Stone's Personal Information Request web form available here: LINK.

Choices with Respect to the Collection and Use of Personal Information

Where required by applicable law, and notably by GDPR, the customers have the right to obtain confirmation of the existence of certain Personal Data relating to you, to verify its content, origin, and accuracy, as well as the right to access, review, port, delete, or to block or withdraw consent to the processing of certain Personal Data (without affecting the lawfulness of processing based on consent before its withdrawal), by contacting the company as detailed below. In particular, the customers have the right to object to Rosetta Stone's use of Personal Data for direct marketing and in certain other situations at any time. Contact Rosetta Stone below for more details. Please note that certain Personal Data may be retained as required or permitted by applicable law.

If the customers are an End User receiving access to Rosetta Stone's services through a Corporate, Governmental, Educational or other Organizational Enterprise Client of Rosetta Stone, and the customers wish to request access, limit use, limit disclosure or remove their End User Personal Data, please contact the Enterprise Client organization that submitted the client's personal data to Rosetta Stone, and Rosetta Stone will support them as needed in responding to the request.

If the customers are contacting Rosetta Stone to request information or action with respect to personal data Rosetta Stone has collected about you, or to exercise their data protection rights, please click HERE and submit their request(s) through Rosetta Stone's Personal Information Request web form.

If the customers have other questions or requests concerning their personal information, please contact the Privacy Team by e-mail at privacyofficer@rosettastone.com.

If the data subjects are a resident of the European Union with questions regarding their rights in Personal Data under GDPR, please contact the Rosetta Stone Data Protection Officer, Sofia Simoes, by e-mail at DPO@rosettastone.com.

(a) As noted above, the customers can choose not to provide Rosetta Stone with personal information, although it may be needed to register as a member on the Service and to participate in certain features offered through the Service.
(b) The customers can access or update their personal information by using Rosetta Stone's Personal Information Request web form available here: link.
(c) The customers may stop the delivery of commercial e-mail communications that Rosetta Stone sends by following the instructions accompanying a particular communication or by using Rosetta Stone's Personal Information Request web form available here: link.
(d) The Help portion of the toolbar on most browsers will tell the customers how to prevent their browser from accepting new cookies, how to have the browser notify the customers when the customers receive a new cookie, or how to disable cookies altogether.

In addition, Rosetta Stone will comply with the mandatory requirements of the applicable laws of any state, federal or other governmental jurisdiction regarding their personal information.

Security

The customers should be aware that there is always some risk involved in transmitting information over the Internet. While no website can guarantee security, Rosetta Stone has implemented reasonable administrative, technical, and physical security procedures to help protect personal information from loss, misuse or alteration by unauthorized third parties. For example, Rosetta Stone maintains policies and protocols to restrict access to personal information only to authorized personnel, and only for permitted business functions.

Transfer of Data

The Internet is a global environment. Using the Internet to collect and process personal Data necessarily involves the transmission of Data on an international basis. For individuals located in the European Union, Rosetta Stone participate in the EU-U.S. and Swiss-U.S. Privacy Shield Framework (the "Framework") as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal data from the European Union and Switzerland. For more information about Rosetta Stone's certification to the Framework, please click here: http://www.rosettastone.com/privacy-shield, or to visit the U.S. Department of Commerce site please click here: https://www.privacyshield.gov/welcome.

Children Using the Service

In the United States, the Children's Online Privacy Protection Act imposes certain restrictions on web sites and online services that are directed at children under 13 or where the operators know that they are collecting personal information from children under the age of thirteen (13). Unless the Service makes specific references to children and collects age information, in which case further required disclosures will be provided, the Service is not directed at or intended for children under 13 years old in the United States or other minimum age specific to certain other countries in those locations. Accordingly, Rosetta Stone will not knowingly collect personal information from children under the required minimum ages through a Service that is not intended for children without the consent of a parent or authorized guardian. Rosetta Stone do not knowingly allow children under the age of thirteen (13) or other required minimum age to publicly post or otherwise distribute personally identifiable contact information through the Service, and Rosetta Stone do not condition the participation of a child under thirteen (13) or other required minimum age in the Service's online interactive activities on providing personally identifiable information. If Rosetta Stone becomes aware that the company have inadvertently received personally identifiable information from a user under the minimum age without the consent of a parent or authorized guardian, Rosetta Stone will use that information to respond directly to that child to inform him or her that the Service is not intended for children under the minimum age, and Rosetta Stone will delete that information from Rosetta Stone's records.

Third-party Websites

Websites to which this Service links do not operate under this Policy. Rosetta Stone recommends that the client examine the privacy statements posted on those other websites to understand their procedures for collecting, using, and disclosing personal information.

Changes to This Policy

Rosetta Stone may update this Policy in the future to reflect changes in Rosetta Stone's privacy practices, Rosetta Stone's website functionality, or applicable legislation, so please check back often. Rosetta Stone will notify the customers about material changes to this Policy by sending a notice to the e-mail address the customers provided to Rosetta Stone or by placing a prominent notice on the Service.

How The Customers Can Contact Us

If the customers have questions about this Policy, please e-mail Rosetta Stone at privacyofficer@rosettastone.com. The customers may request a copy or send a correction of the personal information Rosetta Stone hold about the customers by contacting the Privacy Officer at privacyofficer@rosettastone.com or writing to:

Privacy Officer
Rosetta Stone Ltd.
135 West Market
Street Harrisonburg
VA 22801 USA

If the customers wish to report communications or actions of other users that the customers believe may be in violation of this Policy or Rosetta Stone's Terms of Use, the customers may contact Rosetta Stone by clicking on the "Contact Us" or "Report Abuse" link at the bottom of the Service's webpages.

California Consumers

Notice to California Consumers *This notice is effective as of January 1, 2020*
If the customers reside in California, Rosetta Stone is required to provide additional information to the customers about how Rosetta Stone uses and disclose their information, and the customers may have additional rights with regard to how Rosetta Stone uses the information. Rosetta Stone has included this California-specific information below: • CA Personal Information. Consistent with section 1 of this *Privacy Policy*, Rosetta Stone collect certain categories and specific pieces of information about individuals that are considered "Personal Information" in California ("CA Personal Information"), specifically: o Personal and Other Identifiers or Characteristics: such as first name and last name, personal or professional contact information, mailing address, telephone number, e-mail address, unique personal identifier, IP, device, and online activity information, age, date of birth, gender, demographics, username and password to Rosetta Stone's Websites or services o Commercial Information**:** such as payment details, credit card information and purchase or transaction history o Sources. Rosetta Stone may collect certain categories of CA Personal Information from the customers and other third parties as described in section 1 of this *Privacy Policy* • Use of CA Personal Information. Consistent with sections 2 and 3 of this *Privacy Policy*, Rosetta Stone may use CA Personal Information for business or commercial purposes. Please see sections 2 and 3 for more details • CA Personal Information Sold or Disclosed For Business Purposes o In the preceding twelve months, Rosetta Stone may have shared CA Personal Information for business purposes, or Rosetta Stone may have "sold" (as defined under CCPA) some categories of CA Personal Information • California Consumer Rights. Subject to certain exceptions, as a California resident, the customers may have the following rights to their CA Personal Information: (i) *Access*. Request access to their CA Personal Information that Rosetta Stone may collect, use, disclose, or sell; (ii) *Deletion*. Request deletion of their CA Personal Information; and (iii) *CA Personal Information Sold or Disclosed For Business Purposes.* Request information about the CA Personal Information Rosetta Stone has "sold" (as defined under CCPA) or disclosed for business purposes within the preceding 12 months. To the extent permitted by applicable law, Rosetta Stone may be required to retain some of their CA Personal Information and certain CA Personal Information is strictly necessary in order for Rosetta Stone to fulfil the purposes described in this Privacy Policy

Notice to California Consumers *This notice is effective as of January 1, 2020*
• Exercising California consumer rights**.** If the customers are a California resident and wish to exercise any of these rights, please: (a) submit their request using the California webform available here*;* (b) log into their account to make any updates or submit a request; (c) contact Rosetta Stone as described in the *Privacy Policy* section 12 above, or (d) call the following toll-free number 800-280-8172. When submitting their request, the customers may be asked to provide certain information, which may include additional proof of identification, so that Rosetta Stone can verify their identity and validate the request. Rosetta Stone is not responsible for requests that are not sent or submitted properly, or that do not have complete information. Please note that the customers are limited by law in the number of requests the customers may submit per year. Rosetta Stone will not discriminate against the customers by offering the customers different pricing or products, or by providing the customers with a different level or quality of products, based solely upon the customers exercising their rights to their CA Personal Information • Do Not Sell the Personal Information. If Rosetta Stone "sell" (as defined by CCPA) their CA Personal Information to a third-party, as a California Resident, the customers have the right to opt-out of the sale of their CA Personal Information. If the customers wish to exercise this right, please click here, contact Rosetta Stone as described in the *Privacy Policy* section 12 above, or call the following toll-free number 800-280-8172. To the extent that the customers elect to designate an authorized agent to make a request on their behalf, the customers must identify that they are contacting Rosetta Stone as agent and will be required to provide appropriate documentation including written signed authorization by you, proof of their identity, and verification of their identity; or a valid, designated power of attorney as required under the California Probate Code. Rosetta Stone may require additional proof of authority or may need to contact the customers directly to validate the request. If the customers are under the age of 16, Rosetta Stone will not sell their CA Personal Information without proper consent

Last reviewed: January 1, 2020
Last updated and effective as of: January 1, 2020

Lexia Application Data Privacy Policy

Lexia Learning Systems LLC. ("Lexia", "We", "Us", or "Our") respects their privacy, and strives constantly to earn and keep their trust. All personal information the customers share with Rosetta Stone is treated with the utmost care. Lexia has created this application privacy policy to establish Lexia's commitment to the privacy of their data and the data of their students and children. It describes how Lexia collects, uses, shares and secures the personal information the customers provide. It also describes the choices available to the customers regarding Lexia's use of their personal information and how the customers can access and update this information. The use of information collected through Lexia's service shall be limited to the purpose of providing the service for which the customers (their school or school district), has engaged Lexia.

This privacy policy applies exclusively to the Lexia SaaS-based educational products and associated services, including the website www.mylexia.com (the "Site") and MyLexia mobile application.

1. Information Lexia Collect and How Lexia Use It.
2. Children's Privacy.
3. Sharing Information with Third Parties.
4. Information Security.
5. Changes to This Privacy Policy.
6. Contact Us.

If the customers have an unresolved concern about personal data that Lexia have not addressed satisfactorily, Lexia have committed to cooperate with the panels established by the EU data protection authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) to serve as Lexia's independent dispute resolution bodies for the Frameworks. In addition, under certain conditions, more fully described on the Privacy website, European residents may invoke binding arbitration for non-monetary issues when other dispute resolution procedures have been exhausted.

Lexia receives and processes the personal data of the students, staff and other users of Lexia products and services through service agreements with school and district customers that purchase Lexia's products and services on behalf of those users. Lexia would have no direct relationship with the individual users whose personal data it processes. An individual (user or the user's parent or legal guardian) who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct the query to the school or district or other Lexia customer through which the user receives access to the Lexia product (the data controller). If requested to remove data, Lexia will respond within a reasonable timeframe.

Lexia will retain personal data and process on behalf of Lexia's clients for as long as needed to provide services to Lexia's clients, to comply with Lexia's legal obligations, resolve disputes, and enforce Lexia's agreements.

Software, services and programs delivered and accessed through the Internet necessarily involve the transmission and processing of personal data, sometimes on an international basis, depending, for example, on where the user is located. When personal information is provided to Lexia through the Sites or mobile applications, the information will be processed and stored on servers located in the United States, and by using the Sites and mobile applications, the customers acknowledge and give Lexia authorization to such transfer, processing and storage on behalf of yourself, their organization, and their students or other users as applicable.

Lexia participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. Lexia is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List at https://www.privacyshield.gov/list.

Lexia is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third-party acting as an agent on its behalf. Lexia complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Framework, Lexia is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Lexia may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Under certain conditions, more fully described on the Privacy Shield website at https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, the customers may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Information Lexia Collects and How Lexia Uses It

Lexia collects information, including personal information that the customers provide to us. Lexia also collects personal information when their school or district creates accounts for administrators, teachers, and students. Lexia only collects information that is relevant and not excessive for the purposes for which it is to be processed. Personal information includes information that can identify you. For teachers or administrators, this includes full name, e-mail address, and school. For students, this includes full name, user ID, and school. If the school or district elects to do so, additional optional data may be entered for students that may include demographic data such as gender, birth date, ethnicity, special education, instructional language, participation in free lunch programs, and Title 1 status. This information is only used by Lexia for the purpose of completing the purpose for which provided. Data generated through the use of the Site or mobile application from which personal information and attributes about any user has been removed ("de-identified data"), may be used by Lexia for lawful purposes, including, without limitation, product and service improvement or development, general product and service analysis, benchmarking, development of best practices, and/or educational research or statistical assessment.

When the customers download and use Lexia's mobile application or services, Lexia automatically collects additional information, such as the type of mobile device that is being used, operating system version, and the device identifier (or "UDID"). Lexia do not ask the customers for access or track any location-based information from their mobile device at any time while downloading or using Lexia's mobile application or services.

Links to 3rd Party Sites

Our Site also includes links to other websites whose privacy practices may differ from those of Lexia. If the customers submit personal information to any of those websites, their information is governed by their privacy policies. Lexia encourage the customers to carefully read the privacy policy of any website the customers visit.

Children's Privacy

What information is collected online from children under 13?

Children under 13 access Lexia using a student account. Typically these accounts are established by the student's school or by Lexia using information provided by the school. The minimum information required to create a student account is:

- First Name
- Last Name
- Username
- Grade
- School
- Instructional Language (English or Spanish)

To see a full list of all optional data fields - click here.

Do the customers obtain parental consent prior to collecting information from the child?

No. Student accounts are typically created by teachers or school administrators, or by Lexia using information provided by the school. COPPA and other laws authorize schools to act in place of the parent or guardian in deciding whether to give consent to the collection and use of student information for educational purposes. By creating the student account on the Site, teachers provide consent and authorization for Lexia to store and process personal data about those children for purpose of providing the Lexia program. Children under 13 cannot create their own accounts and parents do not have access to the administrative portion of Lexia's Sites where student accounts are created.

Yes. When Lexia receive or access student personal data and education records from Lexia's school and district customers through their use of Lexia's products and services, Lexia understand that Lexia are acting in the capacity of a "school official" under FERPA, and are committed to complying with the limitations and requirements imposed on Rosetta Stone as an educational service provider to Lexia's school and district customers under FERPA and other applicable state student records privacy laws. Student personal data is used only for the purpose of fulfilling Lexia's duties and provisioning Lexia's products and services under Lexia's services agreement with Lexia's school and district customer, and is not otherwise used or disclosed except as provided for in the service agreement, as required by law, or as authorized or directed in writing by Lexia's school or district customer.

Can a child enter personal information into their Site?

No. Personal information about children can only be entered by school personnel or by Lexia personnel acting on their behalf. There is no way for a student using the Lexia program to enter or store additional personal information on Lexia's Sites. The Lexia program collects and stores data created by student use of the program (namely, reading performance and progress data), which is linked to each student's respective personal information.

Is a child's personal information required for participation in the Lexia program?

Yes. Students need individual accounts to access the Lexia program and so that their progress in the software program can be monitored by the school and its teachers.

Is children's information shared with unrelated third parties?

No. Personal information obtained online from students is not released to any unrelated third-party except as permitted by law or as expressly set forth in this policy (such as to certain Affiliated Businesses, as provided below), or at the direction of the school.

What are the choices of a parent or guardian?

Lexia collects information under the direction of its Clients (school personnel or administrators of the Lexia product), and has no direct relationship with the individuals whose personal data it processes. If the customers are a parent or guardian or otherwise a customer of one of Lexia's Clients and would no longer like to be contacted by one of Lexia's Clients that use Lexia's service, please contact the Client that the parents interact with directly. Service providers that Lexia utilize to provision Lexia's products and services, and who may access or receive personal information to provide those services or functionality, are under contractual obligations with respect to the personal information and are covered by the service agreements with Lexia's Clients.

Parents and legal guardians can make choices regarding the personal information Lexia store online for their children by contacting their child's school to review what personal information is being collected. Parents who experience difficulty or require additional information may contact Lexia directly, however, parents should start by contacting the school first since the school is the entity that contracted with Lexia for the services and authorized the information to be collected and stored. In addition, the child's school be in best position to verify the parent's identity and connection to the student, which would be necessary before Lexia could respond to this type of request.

Upon written request from the school, or from a confirmed parent or legal guardian (as noted above), Lexia will provide an inventory of the personal information it holds on their behalf and take reasonable steps to allow such persons to review their information for the purposes of correction or removal, subject to the limitations (including disproportionate burdens) set forth in the US Department of Commerce's Privacy Shield Principles. Lexia will respond to all inquiries within 30 days of receipt. Please see the contact information provided at the end of this privacy policy to contact us.

Sharing Information with Third Parties

Lexia does not release personal information collected or received in the Sites or mobile application to any unrelated third parties for promotional purposes. Lexia may, however, share aggregated product usage data with unrelated third parties, and share personal information only as described below:

Affiliated Businesses

Lexia may disclose information (including personal information) collected from Lexia's Site with Lexia's local authorized Lexia representatives for sales and support purposes. Lexia require these representatives to comply with this policy. Lexia will not share their contact information with other businesses except service providers and successors, as described below.

Service Providers

Lexia may share their information with Lexia's service providers—that is, organizations providing services to support Lexia functions, such as Lexia's hosting services provider, mail and e-mail processing providers, payment processing providers, and research and support providers. All such service providers are bound by contract to refrain from using the personal information Lexia collect from the customers for any purpose other than providing the specified service to Lexia.

Successors

In the event Lexia is sold to a new owner, whether by merger, stock sale, asset sale or other means, Lexia retains the right to transfer personal information to the new owner, provided notify the customers this is occurring (which may be by posting on Lexia's websites) and the new owner agrees to respect the privacy policy in effect with respect to this personal data.

Laws and Legal Rights

Lexia also may release personal information at the request of law enforcement authorities, when ordered to do so where a formal request has been made such as in a court order, subpoena or judicial proceeding by a court or similar legal process, or when Lexia has the right to do so and believe it is necessary to assert or protect Lexia's legal or intellectual property rights, or in protecting the physical safety of Lexia's employees, users and the general public.

Fraud Prevention

In order to protect Lexia's customers, users and ourselves from fraud or theft, Lexia may provide personal information to law enforcement agencies or to other organizations that agree to respect the privacy policy in effect with respect to this personal data.

Information Security

Lexia utilizes standard security measures, such as firewall, limited access, and SSL encryption technology, designed to help protect against loss, misuse, and alteration of user information collected by Lexia during its transmission. Access to their data is controlled by both physical and logical controls. Only selected members of the Lexia staff can access the raw data on disk or the backup tapes. All backup tapes stored offsite are encrypted and destroyed when they become obsolete. Lexia's production systems are housed in a tier-1 hosting facility that is monitored 24 hours a day, 7 days a week. Access to these systems requires prior written approval from Lexia management and all access is logged and monitored. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, Lexia cannot guarantee its absolute security. If the customers have any questions about security on Lexia's Site, the customers can contact Lexia at privacy@lexialearning.com.

Cookies and other Tracking Technologies

Lexia and Lexia's service providers use cookies or similar technologies. These technologies are used in administering the Site and maintaining user progress within the program, analyzing trends and user movements within the Site, and to gather general usage and demographic information about Lexia's user base as a whole. Lexia may receive reports associated with these technologies by these providers on an individual as well as aggregated basis.

As is true of most websites, Lexia gather certain information automatically and store it in log files. This information may include IP addresses, browser types, referring/exit pages, operating systems, date and time stamps, and "clickstream" data. Lexia do not link this automatically collected data to other information Lexia collect about you.

Teacher and student activity is stored in a relational database and used for reporting and analysis, including student user progress monitoring for teachers and administrators, and aiding Lexia in trend analysis and providing customer support.

Lexia does not give log file information or student usage information to third parties, except (i) those service providers engaged to support and assist in administering Lexia's Sites and mobile application, or (ii) in a sanitized form disassociated from their IP address or other personal data, or (iii) as authorized or directed by the school.

Mobile Analytics

Lexia uses mobile analytics software to allow Lexia to better understand the functionality of Lexia's mobile application software on their mobile device. This software may record information such as how often the customers use the application, events that occur within the application, aggregated usage information, performance data, and where the application was downloaded from. Lexia does not link the information the company stores within the analytics software to any personal user information the customers submit within the mobile application.

Enforcement

Lexia periodically verifies that this privacy policy properly describes the information the company collect and how the company use it, and that the company act in compliance with this policy. Please contact Rosetta Stone if the customers have questions or concerns using the contact information below. The company will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information in accordance with the principles contained in this policy.

With respect to any complaints relating to this policy that cannot be resolved through Lexia's internal procedures, the company will cooperate with appropriate regulatory authorities to resolve such complaints.

Testimonials

From time to time the company may display personal testimonials of satisfied customers on Lexia's Site in addition to other endorsements. With their consent, the company may post their testimonial along with their name. If the customers wish to update their testimonial of request that it be removed, the customers can contact Rosetta Stone at privacy@lexialearning.com.

Social Media Widgets

Our Site includes Social Media Features and Widgets, such as the Facebook button and Twitter button. These features may collect certain information, such as their IP address or which page the people are visiting on Lexia's Site, and may set a cookie to enable the feature to function properly. Social Media Features and Widgets are either hosted by a third-party or hosted directly on Lexia's Site. The customers' interactions with any of these features is governed by the privacy policy of the company providing it.

Changes to This Privacy Policy

Last reviewed: February 3, 2020
Last updated: February 3, 2020

The company may amend this privacy policy at any time. If the company make material changes in the way the company collect, use, and/or share personal information, the company will notify the people by prominently posting notice of the changes on the Sites covered by this privacy policy for thirty (30) calendar days prior to the implementation of the material change and provide instructions on how to remove the customers' information prior to the changes taking effect.

The Customers' Choices and Access to Their Information

Lexia offers those who provide personal information the opportunity to withdraw consent with respect to the information they submitted at any time ("opt-out"), in which case such personal information will not be further processed. Lexia's e-mail programs allow the customers to choose to receive or stop receiving communications from us. The company honor a "once out - always out" policy. Each secondary e-mail the company send to Lexia's recipients contains 'Unsubscribe' instructions. Once the customers opt out, the customers are opted out of that type of communication until the company are explicitly told in writing that the customers want to opt back in. The customers may opt out of e-mail programs at any time by following the Unsubscribe instructions provided in the e-mail the customers receive from us. Upon request Lexia will provide the customers with information about whether the company hold any of their personal information. For the Sites and mobile applications, the customers may access their personal information for the purposes of correcting, amending, or deleting it by logging into their account and reviewing and selecting their profile preferences. The customers may also contact Rosetta Stone to request assistance for which the company will respond to within a reasonable timeframe and as may be required by law.

The General Data Protection Regulation (GDPR) and EU data subjects:

Where required by applicable law, and notably by GDPR for residents of the UK and European Union, the customers have the right to obtain confirmation of the existence of certain Personal Data relating to you, to verify its content, origin, and accuracy, as well as the right to access, review, port, delete, or to block or withdraw consent to the processing of certain Personal Data (without affecting the lawfulness of processing based on consent before its withdrawal), by contacting Rosetta Stone as detailed below. In particular, the customers have the right to object to Lexia's use of Personal Data for any direct marketing and in certain other situations at any time. Please note that certain Personal Data may be retained as required or permitted by applicable law.

Lexia acknowledges that the customers have the right to access their personal information. If the customers are a student or other end user receiving access to Lexia through a school, the customers will need to contact the school administrator that submitted their personal information to us, and the company will support them as need in responding to their request to access, change or delete the personal information submitted and associated with their account. Requests will be addressed within a reasonable timeframe and as may be required by law.

The company will retain their information for as long as their account is active or as needed to provide the customers services. The company will retain and use their information as necessary to comply with Lexia's legal obligations, resolve disputes, and enforce Lexia's agreements.

Contact Us

If the customers have questions or concerns regarding their privacy, please contact Lexia as follows:

Privacy Officer
Lexia Learning Systems LLC
300 Baker Avenue, Suite 320
Concord, MA 01742 U.S.A.
E-mail: privacy@lexialearning.com
Telephone: 1-978-405-6200

If the customers are a resident of the UK or European Union with questions regarding their rights in Personal Data under GDPR, please contact the Lexia Learning Data Protection Officer, Sofia Simoes, by e-mail at DPO@lexialearning.com.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All Company employees are obliged to adhere to the Company's policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Company employee.

Physical Security

Datacenter Security

The Company maintains a physical co-location presence with dedicated cages in facilities in Virginia and Massachusetts. The company also maintains a presence in AWS for server infrastructure and content delivery. The co-location service provider maintains a website where the list of personnel that the Company designates to have cage access permission, is managed and updated by the Company IT designee. Upon arrival at the datacenter, a security guard verifies that the individual is from the Company and verifies that they are on the current access list. The guard verifies full legal name and other information for the individual according to the co-location provider's security protocols. Only once confirmed and validated will the individual be given a temporary access card as well as physical key. The access card grants access to the datacenter itself (through a mantrap), and the key is for the physical lock on the Company's private cage. The above procedures and policies are established, maintained and enforced by the co-location service provider.

The Company has an internal access control policy through internal Company workflows. Company IT team members can request addition or change to the list of Company personnel authorized to access the co-location facilities, which authorization must be expressly approved by the IT manager.

By default, access granted temporarily to the Company's co-location facility expires at midnight of the day it was granted. Temporary access also requires that a co-location facility service provider representative escorts the Company designee during their time in the co-location facility. The co-location facility service provider representative escort may be given an access card, but the service provider escort does not receive the cage key or get physical access to the cage.

Certain Company personnel may receive persistent access and assigned access cards based on need and role in the Company. The official access list is audited quarterly as part of the Company's "Quarterly Access Review" process.

Rosetta Stone Building Security

By Company policy, Company buildings are protected by access card locks on all external entrances, unless and except during times that a Company receptionist is present. Visitors are required to sign in and out with reception and escorted by Company employees while in a Company facility. Each building has video surveillance operated by the Company's Facilities team or building owner. In some locations, the building owner controls an additional layer of access (e.g., guards that check IDs in the lobby and/or parking facilities, additional video surveillance for the building, etc.).

Upon an employee or contractor's termination of employment, the Human Resources Management System (HR Management System) generates an access deletion record in the HR Management System on the last day of employment. This record is routed to Rosetta Stone IT Helpdesk where access is removed. In addition, terminated employees and contractors are required to turn over their access cards/IDs during their last day to their manager or designee.

On a quarterly basis, system owners review access to their system resources. Access listings are generated by Information Technology and distributed to the system owners via the access management system. System owners review the listings and indicate the required changes in the access management record. The record is routed back to the access administrators for processing.

Logical Access

The Company uses permissions-based controls based on principles of least privilege access and requires users of the system to be identified and authenticated by the system owner manager prior to the use of Company systems and resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized security roles in access control lists.

Company resources are managed in the access request system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing regular reviews of access.

Employees and approved contracted personnel sign on to the Company network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval and disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts.

Employees and approved contracted personnel accessing systems from outside the Company network are required to use a two-factor authentication system.

Employees and approved contracted personnel accessing certain internal Company resources from outside the Company network are required to use a VPN with a two-factor authentication system.

Upon hire, employees are assigned to a position in the HR Management System. Prior to the employee's start date, the HR Management System notifies IT to create an employee user ID. Company IT sets the employee access to Company systems based on role of new employee, following access rules that have been pre-defined based on the defined roles. The manager of the new employee and the owner of the system(s) to which the new employee will receive access receive notification and must approve the systems and permissions set up by Company IT within the access control system before access is granted. The HR Management System also provides notification to Company IT, and employee access rights are reviewed and verified, when the employee's position and/or associated roles changes.

On a quarterly basis, access roles and users for each role are reviewed by system owners. In evaluating role access and user access, system owners consider duties requiring segregation and risks associated with access. System owners make adjustments to access as needed.

Upon termination of employment, the HR Management System notifies IT of the terminated employee or employees. Rosetta Stone IT helpdesk removes employee access to Company systems, Active Directory, and provisioned accounts.

Computer Operations - Backups

Language

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on customer indicated preference within the documented work instructions.

Literacy

All web servers can be recreated and have no persistent data stored on them. The database is replicated live to multiple copies in separate locations.

Computer Operations - Availability

Incident response policies and procedures are in place, and reinforced with training, to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon actual or suspected system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

The Company monitors the capacity utilization of physical and computing infrastructure both internally and externally so that service delivery capacity and service level agreements align. The Company evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Data center space, power and cooling
- Disk storage
- Network bandwidth

Patch Management

The Company has implemented patch management processes so that contracted customer and Company infrastructure systems are patched in accordance with vendor recommended operating system patches. Company IT and Product system owners review proposed operating system patches regularly and as patch notifications and recommendations are received from vendors. Company IT and Product are responsible for determining the impact and prioritization of applying or not applying patches based upon the function of the affected systems within the Company architecture, the nature of the data processed, the security and availability impact of those systems, and any critical applications hosted on them. Company IT and/or Product staff validate that all patches have been installed and tested/confirmed, and, if applicable, that any necessary reboots have been completed.

Change Control

The Company maintains a documented Systems Development Life Cycle (SDLC) policy to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Development management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Firewall systems are in place to enable filtering of unauthorized inbound network traffic from the Internet and denial of network connections that are not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized personnel.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Additional Information

The Company conducts periodic and ongoing third-party vulnerability scanning and penetration testing to identify vulnerabilities and assess the effectiveness of the security of the applications and the network. The third-party tools deployed by the Company use industry accepted vulnerability scanning and penetration testing methodologies. Vulnerability scans are conducted from both outside and inside of the Company network. The third-party providers scan the web applications for vulnerabilities and then attempt to exploit the vulnerabilities to determine whether unauthorized access or other malicious activities are possible.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Company policy. The third-party vendor uses industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Company system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Boundaries of the System

The scope of this report includes the Rosetta Stone SaaS and Lexia Learning SaaS Services performed in the Arlington, Virginia; Harrisonburg, Virginia; Concord, Massachusetts; Boulder, Colorado; Seattle, Washington; and London, United Kingdom facilities.

This report does not include the data center hosting services provided by Evoque and the cloud hosting services provided by AWS, GCPS, and Azure at the various facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

Rosetta Stone believes that the effectiveness of controls should model and reflect the integrity and ethical values of the Company and the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the Company's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of the Company's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of Company values and behavioral standards to personnel through policy statements, codes of conduct and training, and by example.

Specific control activities that the service organization has implemented in this area are described below:

- Documented organizational policy statements and codes of conduct that communicate Company values and behavioral standards to personnel
- Employees are required to sign/attest to the Rosetta Stone Code of Conduct, and receive Code of Conduct training at least annually
- Employees receive data privacy and security training at least annually, with additional targeted training delivered to specific business units throughout the year
- Regular Company *Culture of Data Privacy & Security* messaging and reminders are communicated by Company management and Legal to all Company employees throughout each year
- Employees and contractors sign terms of confidentiality committing them not to disclose Company proprietary or confidential information, including the Company's customer and user information, to unauthorized parties, as a condition of their employment/engagement
- Background checks are performed for U.S._employees as part of the hiring process, and are performed annually for certain employees, based on factors such as role and access to sensitive Company data and/or systems

Commitment to Competence

The Company defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the Company has implemented in this area are described below:

- Management considers the competence levels for particular jobs and translates required skills and knowledge levels into written position requirements
- Annual employee performance reviews allow managers the opportunity to discuss and provide feedback on employee skills and opportunities for additional or targeted training and skills development
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

The Company's management philosophy and operating style encompasses a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, personnel, and resource allocation.

Specific control activities that the Company has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held regularly to discuss major initiatives and issues that affect the business as a whole
- Executive leadership regularly reviews and monitors updates from Enterprise Risk Management Team
- Executive leadership is updated on audits performed by internal and external auditors

Organizational Structure and Assignment of Authority and Responsibility

The Company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management supports establishing a relevant organizational structure that includes considerations of key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

The Company's assignment of authority and responsibility include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key personnel, and continual review of resources provided for carrying out duties. In addition, the Company's approach to assignment of authority and responsibility includes policies and communications directed at ensuring personnel understand the Company's objectives, ethics and business practices; know how their individual actions interrelate and contribute to those objectives; and recognize how and for what they will be held accountable.

Specific control activities that the Company has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated and made readily accessible to employees
- Organizational structures and roles are regularly reviewed by Company Executive leadership and updated as needed to meet the Company's business goals

Human Resource Policies and Practices

Rosetta Stone's success is founded on sound business ethics, and reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel to support the Company's ability to operate at maximum efficiency. The Company's Human Resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the Company has implemented in this area are described below:

- Background checks are performed for U.S. employees as part of the hiring process, and re-performed annually for certain employees, based on factors such as role and access to sensitive Company data and/or systems
- New employees are required to sign acknowledgement forms for the Rosetta Stone Code of Conduct, as well as a confidentiality agreement
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in the HR Management System

Risk Assessment Process

The Company has established an Enterprise Risk Management Team that reviews, monitors and reports to the Executive Leadership on risks at the enterprise level and including all areas of the business.

The Company's risk assessment process identifies and assesses risks that could potentially affect the Company's ability to provide reliable services to its enterprise and consumer customers and learners. This ongoing process requires that management identify significant risks inherent in products, services or operations as they oversee their areas of responsibility. The Company Enterprise Risk Management Team works to identify the underlying sources of risk, measure and assess the potential impact to the Company, and support Executive leadership in establishing acceptable risk tolerance levels and in identifying and implementing appropriate measures to monitor and manage identified risks.

This process is designed to enable the Company to identify risks resulting from the nature of the services provided by the Company, and to support management in identifying and implementing measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance risk - legal and regulatory changes

The Company utilizes an internal auditor and an Enterprise Risk Management Team responsible for identifying risks to the Company and monitoring the operation of the Company's risk internal controls and mitigations measures. The approach is intended to increase visibility and focus of management on enterprise risks, to align the Company's strategy more closely with its key stakeholders, to assist the organizational units with managing uncertainty more effectively, to minimize threats to the business, and to maximize the Company's preparedness for and opportunities in the rapidly changing market environment. The Company attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of the Company with respect to its product and service offerings; as well as the nature of the components of the system and threats from external factors, all result in potential risks to the Company and the security of its systems and operations. The Company addresses these risks through the implementation of suitable compensating controls or measures designed to provide reasonable assurance that Company standards and protocols are maintained. Because each system and the environment in which it operates are unique, the combination of risks to meeting the Company standards, and the controls necessary to address the risks, will be unique. As part of the design and operation of the system, the Company's management works to identify these specific risks to better enable the system owners to identify and implement the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of the Company's internal control system. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the Company's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Rosetta Stone, information is identified, captured, processed, and reported by various information systems, as well as through communications with clients, vendors, regulators, and employees.

Various quarterly, monthly and weekly meetings are held to discuss operational efficiencies within the applicable functional areas and to develop, disseminate new policies, procedures, controls, and other strategic initiatives within the organization. General updates to Company-wide security policies and procedures are typically communicated to Rosetta Stone personnel via e-mail messages, posting on the Company Intranet Site, and through targeted training sessions.

Monitoring Controls

Management oversees the monitoring of controls to ensure that they are operating as intended, that controls are modified as conditions change, and that the quality of internal controls continues to be monitored over time. Necessary corrective actions are taken as required to correct identified deviations from Company policies and procedures. Employee activity and adherence to Company policies and procedures is also monitored. This process is accomplished through a variety of ongoing monitoring activities, including, but not limited to, separate evaluations, regular training and regular departmental/manager reviews, and monitoring of Company reporting hotlines.

On-Going Monitoring

The Company's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in the Company's operations at all levels helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances where suspected control breakdown is suspected or identified. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the Company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of the Company's personnel in line with Company policies and standards.

Reporting Deficiencies

Internal tracking is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of identified risks. Risks receiving a critical rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Risk meetings are held quarterly for management to review reported deficiencies and corrective actions.

Changes to the System Since the Last Review

Rosetta Stone's Literacy Division began to move service and content workloads away from the co-location facility in Massachusetts to AWS during the reporting period. The Literacy division plans to exit the Massachusetts co-location by February 2020.

Incident Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common, Confidentiality and Privacy criterion was applicable to the Rosetta Stone SaaS Services System.

Subservice organizations

This report does not include the data center hosting services provided by Evoque and the cloud hosting services provided by AWS, GCPS, and Azure at the various facilities.

Subservice Description of Services

Evoque provides the data center hosting services, which includes physical security controls to protect the systems in scope. Azure, GCP, and AWS provide the cloud hosting services that include physical security controls as well. Refer to subservice organization tables below.

Complementary Subservice Organization Controls

Rosetta Stone's services are designed with the understanding that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to Rosetta Stone's services to be solely achieved by Rosetta Stone control procedures. Accordingly, subservice organizations, in conjunction with the services, are responsible for establishing their own internal controls or procedures to complement those of Rosetta Stone.

The following subservice organization controls are implemented by AWS, Azure, GCPS, and Evoque to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC6.4	Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Security	CC6.4	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Physical access to the datacenter is reviewed quarterly and verified by the datacenter management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.

Subservice Organization - Google Cloud Platform Services		
Category	**Criteria**	**Control**
Security	CC6.4	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
		Annual data center security reviews are performed, and results are reviewed by executive management.
		Physical security measures in place include: • Existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews • Data center entrances have a perimeter security system consisting of badge readers or biometric access system • Data centers utilize a badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building • All emergency exit points from the raised floor are alarmed • Badge reader and biometric access control systems are secured in a restricted space and no physical access to them from public spaces exists • Visitors to the datacenter facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit • Video cameras exist to monitor building entrances, exits, and the areas immediately surrounding the building • At least one security guard is on-site 24x7

Subservice Organization - Google Cloud Platform Services		
Category	**Criteria**	**Control**
		• All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place • All Google cages, suites, and private rooms are secured using either lock/key, badge access control, or biometric access controls • A key sign out sheet and/or log of badge reader activity exists and covers access to Google spaces

Subservice Organization - Evoque		
Category	**Criteria**	**Control**
Security	CC6.4	IDC visitors accessing customer cages are required to sign in at the reception desk, display a visitor badge, and must be escorted into the buildings by security personnel.
		Requests for physical access to areas within the GCSCs and IDCs are granted on the basis of employee or contractor's job responsibilities.
		Requests for physical access are authorized by the employee or contractor's supervisor or manager.
		Physical access to the IDC data center is limited to pre-authorized employees and customers. For individuals who are not on the permanent access list, temporary access is arranged by authorized managers or authorized customer personnel and communicated to the IDC Operations or Security team.
		Security personnel compare customer/vendor/visitor picture IDs to records of individuals on the permanent access list or pre-authorized temporary access requests before allowing access to the IDC.
		Authorized customer personnel or contractors accessing the IDC must sign in and out on the appropriate access log.
		Physical access to the IDCs is controlled by physical barricades or mantraps (subject to local building code requirements) between the reception area and the actual data center. The barricade is activated by the use of a card-key access system.
		Customer hardware systems are physical separated from other hardware in locked cabinets or cages.
		All individual customer facilities are physically secured using separated locking cabinets and/or cafes depending on the physical equipment size requirements.
		Authorized individuals are provided with a cardkey for physical access within the facilities with access rights as defined for a customer or by the job description of the facility employee.

Subservice Organization - Evoque		
Category	**Criteria**	**Control**
		Customer additions or removals from the permanent access list are performed either through the Business Direct Portal or Remote Hands Ticket, submitted by authorized customer personnel. Removals are communicated by sending an Access Change Control Form to the IDC Operations or Security team.
		When a contact is removed from the permanent access list by an authorized requestor for a U.S. IDC, the IDC Operations or Security team retrieves the contact's card-key or disables the contact's cardkey in the card access database.
		Systems used to monitor customer networks are housed in physically secure facilities, with door access controlled by a card-key system.
		Employees and contractors are provided with physical access only to areas to which they are authorized, based on approval procedures. Access to sensitive areas is segregated from other areas and is controlled by the use of electronic access controls.
		Access to facilities and sensitive areas is controlled using an automated card-key system.
		Employee and contractor physical access rights to the GCSCs and IDCs are removed upon termination notification.
		The network environment is designed to logically segregate each customer's network assets. Customer networks are also segregated from the Internal network.

Rosetta Stone management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as service level agreements. In addition, Rosetta Stone performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with subservice organizations
- Making site visits to subservice organizations' facilities
- Testing controls performed by subservice organizations
- Reviewing service-related communications and attestation reports about services provided by subservice organizations
- Monitoring external communications, such as industry reports and customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Rosetta Stone's services are designed with the understanding that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Rosetta Stone's services to be solely achieved by Rosetta Stone control procedures. Accordingly, user entities, in conjunction with the services, are responsible for establishing their own internal controls or procedures to complement those of Rosetta Stone.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities and their auditors should exercise judgment in selecting and reviewing their complementary user entity controls.

CC6.0 - Logical and Physical Access Controls:

1. User entities are responsible to ensure that they timely notify Rosetta Stone regarding changes to their enterprise administrator accounts.
2. The user entities/customer entities are responsible for maintaining the security of their accounts.

CC7.0 - System Operations:

3. User entities are informed of the minimum systems and technical requirements necessary for the Company solutions to operate and are responsible for maintaining their own systems to at least the minimum required settings, versions, and patches as per contractual agreements.
4. User entities must notify Rosetta Stone of any suspected violations of the Company License Agreement by their users, including shared enterprise administrator or user access credential information, security breaches, or compromised user accounts that interact with Company products and/or that perform data/files transfers to or from the Company.

Privacy:

5. The enterprise customer administrators (where applicable) for user accounts are responsible for ensuring that they maintain the accuracy of their user accounts, for managing their users' licenses and access, and for removing and contacting the Company operations teams regarding removal of their terminated users as per contractual agreements.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to all Security, Confidentiality and Privacy Categories)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy

Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Although the confidentiality applies to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized as follows:

i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. *Collection.* The entity collects personal information to meet its objectives related to privacy.

iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

vii. *Quality.* The entity collects and maintains accurate, up-to date, complete, and relevant personal information to meet its objectives related to privacy.

viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Control Activities Specified by the Service Organization

The applicable trust criteria, risks, and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing them in this section. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Rosetta Stone's description of the system. Any applicable trust services criteria that are not addressed by control activities at Rosetta Stone are described within Section 4 and within the Subservice Organization section above.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.