

STUDENT RECORDS PRIVACY STATEMENT & SECURITY PLAN

Rosetta Stone Ltd.

We take the privacy of our educational clients and student users seriously, and we understand the need to safeguard personally identifiable information in records of students who access and use our web-based language and learning products and services (“Student Records”) through the educational institutions, schools and school districts that we serve (our “Education Clients”).

Student Records are the property of our Education Clients. We receive those Student Records solely for the purposes of delivering our products, services and commitments under our agreements with our Education Clients. We are committed to working with our Education Clients to comply with all applicable laws, rules and regulations governing the use and protection of Student Records, including the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and its implementing regulations, and applicable state laws and statutes governing Student Records. As such, we commit to implementing and maintaining this Student Records Privacy Statement & Security Plan (“Student Records Security Plan”), which is designed to protect the security, confidentiality and integrity of Student Records that we receive from our Education Clients, and protect against unauthorized access or other anticipated threats to those Student Records.

In connection with our Student Records Security Plan, we maintain administrative, technical and physical safeguards designed to secure Student Records both during transmission and while in our custody. These safeguards include technical and operational measures, such as firewalls, routers, encryption, passwords, and vulnerability testing, as well as training, policies and procedures to limit access to Student Records to authorized staff, contractors and agents that have a legitimate need to access such data for purposes of delivering and supporting our products and services to our Education Clients, and that are under appropriate contractual obligations of confidentiality, data protection and security.

We utilize various authorization and authentication technologies and processes to limit access to Student Records to authorized persons, including: (i) granting access rights on the basis of the least privilege, “need-to-know” principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords with appropriate complexity, length and duration requirements; and (iv) encrypting and logging access to facilities with systems containing Student Records. We provide regular training on our information security and data policies and procedures to our personnel who are responsible for or have access to Student Records. Our products and services do not currently utilize or enable students to upload student-generated content, but if we offer such functionality in the future, we will work in good faith with our Education Clients to develop processes to address requests by students for the transfer of such content generated by the student during the service term.

We use Student Records only for the purpose for which they are provided to us or as otherwise authorized in the applicable agreement with the Education Client. We do not sell Student

Records or use them for targeted marketing or similar commercial purposes, and do not authorize others to do so. We do not disclose Student Records to unauthorized third parties without the permission from the Education Client, unless required by statute, agency or court order, subpoena or similar compulsory legal process.

If a parent, legal guardian or student contacts us with a request to review the user's Student Records or correct erroneous information, or if an agency, court, law enforcement or other entity contacts us and requests access to Student Records, we will (unless prohibited by writ or compulsory legal process) promptly notify an authorized representative of the applicable Education Client and use reasonable and good faith efforts to assist the Education Client in fulfilling such requests, as required by law and directed by the Education Client.

If we determine that an incident involving Student Records has occurred that would be subject to reporting under applicable federal or state law, we will take prompt and appropriate steps to mitigate the incident and/or further impact to the Student Records; provide notice to the affected Education Client promptly and without unreasonable delay; and work with the affected Education Client to provide information and assistance necessary to comply with any notification to parents, legal guardians, students, or other persons or entities, as required under applicable law.

Following expiration or termination of the agreement under which the Education Client purchased access to our web-based products or services and upon receipt of written direction from the Education Client, we will take steps to destroy, or if agreed, return the Student Records in our possession to the Education Client within a commercially reasonable period of time. For clarity, data or data elements within Student Records generated by use of our products or services that are in aggregate form or that are de-identified or anonymized (i.e., where direct and indirect personally identifiable identifiers that would associate the data or element with an individual student or user have been removed), may be retained and used for product and service improvement, statistical analysis, and/or educational research-related purposes.

This Student Records Security Plan is effective March 31, 2016. From time to time we may update this Student Records Security Plan to reflect changes to our privacy practices in accordance with changes in legislation, best practice or our products. Notice of material changes to this Student Records Security Plan will be provided to Education Clients by email to the address on file for the account, by including a notice in our invoice documentation to Education Clients, or by placing notice within our web-based products or on our website.

For questions or further information on our data privacy and security practices with respect to Student Records, please contact our privacy officer at PrivacyOfficer@RosettaStone.com.