DiLL Data Collection and Access Policy

SWIFT EDUCATION SYSTEMS INC. — LAST UPDATED MAY 10, 2019

Overview

DiLL is a software application for language lab activities. In the course of using the software, a limited amount of personally identifiable information about DiLL users is collected and stored on the DiLL server. This personal information generally **remains on-site and fully under the control of the school.**

The DiLL Classroom Software

The DiLL classroom software includes speaking and listening features, which require access to the microphone.

DiLL also provides classroom management features, including screen locking and controlling student computers. Teachers can listen in, lock, view, and control screens of students:

- when they are logged into the same virtual classroom, and
- when they are both on the campus network.

DiLL does not access the camera or location services.

Your DiLL Server

In order to use the classroom applications, a DiLL server ("your server") is hosted on the school network. Your server resides on school premises under the full control of school IT, which is responsible for the physical and network security of your server.

When the DiLL classroom software is used, your server collects students' voice recordings and associated metadata, including student names, user IDs, and login times.

Your server also collects information about the computers the DiLL classroom software is installed on, including serial number, MAC address, the type of headset used, hostname, last IP address, DiLL software version, operating system version, login times, and usage logs.

For support purposes, including diagnosing issue reports and addressing other user requests, Swift Education staff may collect data from your server, which may include student information. This data is deleted by Swift Education when the support issue is resolved.

Data Reported to Swift Education

The DiLL server periodically connects to the Swift Education support server to check for software updates and refresh its software license information. The DiLL server submits to the support server information necessary to track DiLL computers for licensing purposes and to survey which operating system versions are in use.

No computer hostnames, student names, or user IDs are included in these reports. **User information stays on your server.**

Data Security

On-site traffic and data storage

DiLL supports encrypting traffic between the classroom software and server. To enable this feature, please add a valid TLS (SSL) certificate to your server. Self-signed certificates are not supported.

DiLL also supports TLS encrypted connections (LDAPS) to your LDAPv3 authentication host. CA-signed and self-signed certificates are supported.

At the discretion of your IT staff, FileVault can be used to encrypt the disk on your server.

Off-site access via DiLL Connect

The DiLL support plan includes access to the DiLL Connect proxy service, which enables off-site access to the server for the following purposes:

- access to the DiLL website, for teacher review of student recordings, and
- access to screen sharing and secure shell services, for issue diagnostics and other support requests.

The DiLL Connect proxy service is end-to-end encrypted with HTTPS and SSH tunneling. This service can be disabled upon request. The DiLL Connect server retains logs of the IP addresses of connecting clients, and no other identifying information.

The Swift Education support server

The Swift Education support server is hosted in a secure colocation facility and is kept up-to-date with operating system updates and security patches. Automated backups of this system are client-side encrypted prior to being uploaded to cloud storage servers.

Data reported by your server to the support server is sent over an encrypted HTTPS connection.