Frequently Asked Questions: Vivos Online Registration Privacy Policy

Where and how is the data stored?

Hosting of Vivos servers and the related Surrey Schools' data takes place in Canadian Microsoft Premiere Data Centers. Multiple layers of security are in place as per specifications in Premiere hosting services including advanced protection for physical entry, monitoring, and access.

Backups are also stored in Canadian Microsoft Premiere Data Centers and encrypted using Microsoft Azure Backup.

How long is the data stored for?

This data is destroyed annually in compliance with the data destruction guideline provided by Surrey Schools Privacy Officer, and the Director of Information Management Services, District Principal, Student Information Services. The guideline states that data will be removed from district systems once per year as it ages past 1 year (1year + a day). This guideline also applies to data stored on the Vivos server and its removal will be the responsibility of the District Principal, Student Information Services.

In the event that Surrey Schools makes a future decision to cancel its Vivos subscription, Vivos will securely delete District data within 90 days of termination of the contract.

Who has access to the information?

Data access is limited to authorized users and monitored at both the district level and by Vivos personnel.

Data that is downloaded by authorized staff is stored on local servers and the data is only accessible to authenticated District users.

Access to data on Vivos relies on security policies policed through Active Directory Management by IT personnel in Surrey Schools. Only a limited number of IT staff have access to modify security privileges. Access control for Surrey Schools (User) is an automated process that follows the separation of duties principle and the principle of granting least privilege. User Access is limited by user role. For example, authorized users at the school level can only see their own school data. This is accomplished by synchronizing access through Azure Active Directory Services and the District owned and managed Active Directory.

How is it secured?

Data is protected by Azure Data Protection Services. A full white paper explaining the service is available here.

Client communication protocols include transmission from client to server using Secure Socket Layer as well as security provisioning provided by Microsoft. Data is accessed through an encrypted 256-bit Secure Socket Layer (SSL).

Data on the internal production SQL server is encrypted in its static state and is protected behind a firewall. Authentication is in place for all internal and external access.

Prior to adopting the Vivos system, Surrey Schools contracted with IBM Canada to complete a comprehensive Privacy Impact Assessment (PIA). That PIA is reviewed annually by a District privacy consultant and revised as appropriate.

Where can I learn about Surrey's general privacy practices?

Click here for more information on Surrey Schools policies and regulations related to privacy.

Who can I contact if I have more questions?

You can contact us at privacy@surreyschools.ca