Resources for Remote Proctoring Tools

Privacy and Security Terms Negotiated by Queen's University with Verificient for Proctortrack

Queen's negotiated an agreement, dated 28 August 2020, with Verificient for the use of its Proctortrack remote proctoring service. Included in the agreement is a requirement that Verificient update its legal documentation by 15 September 2020, notifying students that the terms published on its website might differ from those negotiated with the student's institution. Accordingly, the Terms of Service and Privacy Policy include the following language:

> **Terms of Service** (https://www.proctortrack.com/terms-of-service/) updated 15 September 2020
>
> - "Unless your Test Sponsor – Academic Institution or other Sponsor Organization, has negotiated separate Terms, (please check with them if you are unsure), the Terms contained in this document are the Terms which apply to your use of our services."
>
> **Privacy Policy** (https://www.proctortrack.com/privacy-policy/) updated 15 September 2020
>
> - "Unless your sponsor institution or organization has arranged separate terms and provided you those terms in writing, or you have been provided different terms in writing by us, the terms of this policy apply to you and your relationship with us."

Furthermore, Queen's agreement with Verificient includes the following clause: "Where there is a discrepancy between what is on the website, and what is on this document, this document will govern."

The following outlines the privacy and security terms negotiated by Queen's with Verificient with respect to students' use of Proctortrack.

Item	Queen's Terms in Negotiated Agreement
Definition of "personal information"	Personal information is defined as "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (including an identification number, location data or online identifier such as an IP address or a cookie identifier)." (Note: Privacy Policy defines personal information as "any information, such as name or email address, that identifies or can be used to identify the person to whom such information pertains, or is associated with a person.")
Collection of personal information	Verificient shall not directly or indirectly collect any personal information for any purposes not authorized by Queen's. Verificient has no ownership of the personal information.
Use of personal information	Verificient will use the personal information for the purpose of supplying the Services and for no other purpose.
Disclosure of personal information	Verificient will not disclose personal information for any purpose not authorized by Queen's. Only those employees and agents of Verificient who require access to personal information to fulfill the services under the agreement shall have access to such information, and all such employees and agents shall have entered into a confidentiality agreement with Verificient.
Storage location	Data is stored in Canada in a Google Canada data centre.
Retention and disposal	Exam data / identity verification sessions are retained for 60 days after which they will be automatically purged, and permanently and irretrievably destroyed in a secure manner. Baseline profile data including biometric data will be retained for up to 365 days and purged after that duration. (Note: Terms of Service say exam data / identity verification sessions held for 180 days after which it will be automatically purged.)
Destruction of data	Queen's can request destruction of any Client data any time prior to the scheduled purge date and Verificient will permanently and irretrievably destroy all personal information (including, but not limited to, student profile/ registration information) held in any format no later than 30 days following such request.

Governing law	The governing law is Ontario and Canada. Verificient must abide by privacy laws including Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), and must assist Queen's meet its obligations under Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA).
Security standards	Verificient, and its subcontractors, shall, in accordance with industry best practices, implement, use and maintain the most appropriate administrative, physical and technological security measures and procedures to fulfill its obligations with respect to ensuring the security and integrity of the personal information.
Security audits	Verificient will conduct annual independent third party audits of its security measures and information handling practices, and upon request, provide the results to Queen's. Verificient is required to prepare an annual Type II System and Organization Controls Report (SOC2).
Breach notification	Verificient must notify Queen's of a breach within 24 hours.
Use of de-identified data	Verificient cannot use de-identified personal information for its own purposes unless it removes all direct and indirect personal identifiers including, but not limited to, name, ID numbers, demographic information, biometric information, and location information. Verificient cannot attempt to re-identify de-identified data or transfer de-identified data to any party unless that party agrees not to attempt re-identification. (Note: Verificient has not indicated any intention to use de-identified data but Queen's included this clause as a precaution.)
Insurance	Verificient warrants it has computer security and privacy liability insurance.
Assignment	Verificient cannot assign the agreement without the prior written consent of Queen's.