ProctorU Security & Privacy FAQ
See below for commonly asked questions and answers concerning security & privacy when using ProctorU.

What information does ProctorU collect during LogMeIn sessions?
ProctorU requires a test-taker to download LogMeIn to secure their digital environment so a password may be entered to launch their exam. LogMeIn is not used to pull information other than the test-taker’s basic system information to ensure that we can successfully proctor exams. Students are asked to “accept” a request during the start process to allow the proctor remote access. In most cases, the proctor will not need access to a test-taker’s computer after the exam begins. If a proctor does need to access a test-taker’s computer during an exam (i.e. technical issue, the student loses access to the exam, etc.), the proctor will communicate the need to the test-taker and prompt the test-taker to allow access to their computer. A proctor is unable to remote into a test-taker’s computer without the test-taker granting permission.

ProctorU’s privacy policy states that they share personal information with Google analytics, Freshmarketer and other third parties for targeted advertising. Can I opt out of this?
ProctorU uses Google Analytics and Freshmarketer to help understand how users are using our services, but not for targeted marketing purposes. There is a link on ProctorU’s privacy page here that allows students to opt out of Freshmarketer tracking.

I am concerned that I have to provide my personal information to a third-party vendor and forced to accept terms and conditions where the vendor is not held liable for certain actions (data leakage, FERPA violations, identity theft, etc). How is my personal information protected?
The only information ProctorU collects is basic directory information (name, email address, physical address, and phone number). Other personal or sensitive information is not collected. ProctorU has multiple walls in place to prevent data breach. ProctorU maintain's strict adherence to industry security standards and regular system checks such as third-party penetration tests and active monitoring to prevent breach.
To date, ProctorU has never had a breach, and no data processed on ProctorU's systems has been compromised in any way.

*If you’d like more information, you can send any questions directly to compliance@proctoru.com*