Privacy is central to the Respondus Monitor architecture. It minimizes the personal data being collected, uses an automated system to analyze it, and then restricts access to the results.

**Privacy by Design**
Respondus Monitor puts privacy and security ahead of product features - always.

**Data Ownership**
Proctoring data is owned and controlled by the university, not Respondus.

**Automated**
Respondus Monitor is a fully automated solution. Only instructors see the proctoring results.

**Compliance & Certification**
Respondus Monitor meets the security requirements of FERPA, GDPR, CCPA, Privacy Shield, and SOC 2 certification. Respondus engineers are AWS Certified.

---

**WHAT WE DON’T DO**

- Don’t require students to register at a Respondus website
- Don’t have students provide an email, password, or address
- Don’t link students with a 3rd-party identification service
- Don’t store biometric profiles on our servers
- Don’t watch students live while taking exams
- Don’t “drop in” on students during an exam
- Don’t review videos after the exam
- Don’t cross-reference network or location data of student
- Don’t sell or share data (it’s the institution’s data, not ours)
- Don’t store student grades on Respondus servers
- Don’t access files or data on the student’s computer
- Don’t do anything on the computer when our proctoring system isn’t in use

---

**WHAT WE DO**

- Integrate seamlessly with the institution’s learning system
- Extend the features of the online testing system already in use
- Turn off the webcam automatically when an exam is completed (or exited)
- Allow institutions to select their own retention policy for proctoring results and exam videos
- Encrypt all data from start to finish
- Require all proctoring results and videos to be accessed via the learning system
- Track all database access by Respondus staff using AWS CloudTrail

respondus.com/privacy