

Top 12 EdTech Data Protection Controls:

- Does the vendor have evidence of annual professional, external security and privacy auditing?
- Is there a complete inventory of suppliers and contractors used to secure the vendor's supply chain?
- Is there evidence of a tested mechanism for the secure disposal of student data?
- Can the platform's controls be trusted to avoid the overcollection or aggregation of sensitive data?
- Is there a standardized framework in use for the protection of data, from the SDLC to the enforcement of policies?
- Does the educational institution collaborate with the vendor on annual incident response testing based on real scenarios?
- Do parents receive direct notice requiring them to provide informed consent to collect, use or disclose children's data?
- When using the Web on school computers are all trackers, ads and non-educational content blocked?
- Is express consent used to inform parents/guardians when student (meta)data is accessed beyond 3rd parties?
- Can all students understand the privacy policy of the school, and validate or verify data protection practices themselves?
- Are monitoring controls in place to immediately detect all unauthorized access to student data and subsequent abuses?
- Are board administrators and educators aware that they are accountable for any adverse outcomes of their edtech use?

