



Safeguarding the Privacy and Security of Protected Data

Policy Statement

ECRA complies with applicable federal and state laws and/or regulations with respect to privacy and data security governed by FERPA and the Protection of Pupil Rights Act (PPRA) and secures all personally identifiable information (PII) in accordance with best practices within the educational technology industry to protect student data from unauthorized disclosure or acquisition by an unauthorized person.

ECRA has the following PII policies:

- ECRA does not disclose PII to ECRA employees who do not have a legitimate educational interest in the PII given the scope of his/her employment at ECRA.
- ECRA employees who access PII have been trained on the recognition and requirements for handling PII in accordance with federal and state laws.
- ECRA de-identifies data when it is no longer needed for the purpose for which it was obtained.

Authentication: User data on our database is segregated by account-based access rules. User accounts have unique usernames and passwords that must be entered each time a user logs-on. The portal issues a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the password of the user.

Advanced Encryption Standard (AES) Algorithm: 256-bit Organizational Validation (OV) Certificate

Passwords: User passwords have complexity requirements and are encrypted.

Physical Security: All servers and infrastructure are hosted in datacenters with 24x7 monitoring, cameras, visitor logs and biometric entry authentication.