

EXPATiate COMMUNICATIONS

Data Security & AI Privacy Policy

For K-12 Special Education Data | Protecting Students, Empowering Educators

Version 2.0 • Effective: 2025 • Reviewed Annually

Our Commitment

At Expatriate Communications, we believe that every student's data is sacred. We are committed to the highest standards of security, transparency, and privacy protection for all student information — particularly for students with disabilities whose records carry the most sensitive and federally protected data under IDEA and FERPA. This document describes exactly how we protect your data, the standards we follow, and the answers to the questions that matter most to you.

1. Data Security Architecture

1.1 Encryption: Data at Rest

All student data stored on Expatriate Communications systems is encrypted at rest using AES-256, the same cryptographic standard used by the U.S. Department of Defense and the financial services industry. This applies to:

- All production databases holding student records, IEP data, evaluation reports, and behavioral intervention plans
- File storage systems containing uploaded documents, assessments, and reports
- Backup media and archived data sets
- Any replicated or disaster-recovery copies of data

1.2 Encryption: Data in Transit

All data transmitted between users, applications, and our infrastructure is encrypted using TLS 1.2 or higher (TLS 1.3 preferred), ensuring that data is unreadable to any party that may intercept network traffic.

- All API communications use HTTPS with certificate pinning where applicable
- Email notifications containing any student-related information use encrypted transport (STARTTLS / DANE)
- End-to-end encryption is applied for any data shared between our platform and third-party integrations
- All internal service-to-service communications inside our infrastructure use mutual TLS (mTLS)

🔒 End-to-End Guarantee: Student data stays encrypted from the moment it leaves your device until it is decrypted and displayed on the authorized recipient's screen. At no point in transit or storage is unencrypted student data accessible to unauthorized parties.

1.3 Access Controls & Identity Management

- Role-Based Access Control (RBAC): Access to student data is granted on a strict need-to-know basis. LEA administrators, case managers, service providers, and support staff each have role-specific permissions.
- Multi-Factor Authentication (MFA): Required for all administrative accounts and strongly recommended for all user accounts.
- Single Sign-On (SSO): Support for SAML 2.0 and OAuth 2.0 federation with LEA identity providers, reducing credential sprawl.
- Least Privilege Principle: Every user account and system service is granted the minimum permissions necessary to perform its function.
- Session Management: Automatic session timeouts, concurrent session controls, and full audit logging of all authentication events.
- Privileged Access Management (PAM): All privileged (admin-level) access is monitored, time-limited, and subject to just-in-time provisioning.

1.4 Infrastructure & Network Security

- Cloud hosting on SOC 2 Type II and FedRAMP-authorized infrastructure
- Virtual Private Cloud (VPC) with network segmentation isolating production, development, and backup environments
- Web Application Firewall (WAF) to detect and block injection attacks, XSS, and other OWASP Top 10 vulnerabilities
- Intrusion Detection and Prevention Systems (IDS/IPS) with 24/7 monitoring
- DDoS protection and rate limiting on all public-facing endpoints
- Regular third-party penetration testing (minimum annually) and continuous vulnerability scanning
- Zero-trust network architecture: no implicit trust based on network location

2. AI Usage & Student Data Protection

Expatriate Communications incorporates AI capabilities to help educators, providers, and administrators work more effectively for students with disabilities. Our AI pipeline is designed with a privacy-first architecture that ensures student PII is never exposed to AI models or third-party AI vendors.

2.1 Our AI Data Pipeline

Before any data touches AI processing, it passes through our privacy-preserving pipeline:

STEP	PROCESS	WHAT THIS MEANS
------	---------	-----------------

1	Sanitization	All raw data is scrubbed for known PII patterns (names, DOB, SSN, diagnosis codes, addresses, SSID numbers, parent contact info) before processing.
2	Tokenization	Each PII element is replaced with a unique, opaque token (a meaningless placeholder). The mapping between real data and tokens is stored in a separate, access-controlled vault.
3	AI Processing	Tokenized — and therefore non-identifiable — data is passed to AI models. The AI only sees tokens, never real student information.
4	De-tokenization	Results are returned from AI with token references. De-tokenization happens exclusively in the secure client layer, on the authorized user's session.
5	Display	The final, complete information is rendered for the authorized user. Real PII is only ever reconstituted at this last step, in a secure, authenticated session.

2.2 What We Will NEVER Do with Your Data

✗ Train AI Models

We do not use any student data, identifiable or otherwise, to train, fine-tune, or update any AI model — whether our own or any vendor's AI platform.

✗ Sell or Share for Profit

We do not sell student data. We do not share student data with advertisers, data brokers, or any commercial entities.

✗ Use for Unauthorized Purposes

Student data is used solely to deliver the contracted educational services. It is never repurposed for analytics, product improvement, benchmarking, or any purpose outside the LEA's agreement.

✗ Expose PII to AI Vendors

Tokenization ensures that even if a third-party AI vendor's system were compromised, no student PII would be at risk — because it was never sent to them.

✗ Retain Beyond Authorized Periods

Data retention schedules are enforced per LEA agreement, FERPA requirements, and applicable state law. Data is securely deleted upon contract termination.

3. Regulatory & Compliance Framework

Expatriate Communications designs its entire data handling infrastructure to comply with all applicable federal and state laws governing student privacy and data security. Below is our core compliance framework.

3.1 Federal Regulatory Compliance

FERPA

Family Educational Rights and Privacy Act. We restrict data access to school officials with a legitimate educational interest, prohibit unauthorized disclosures, and honor parental inspection and amendment rights.

COPPA

Children's Online Privacy Protection Act. For students under 13, we do not collect, use, or disclose personal information without appropriate school or parental consent.

4. Operational Security Practices

4.1 Vendor & Third-Party Risk Management

- All third-party vendors with access to student data are subject to security assessment before onboarding
- Vendors must sign binding Data Processing Agreements and Business Associate Agreements (BAA) where applicable
- Third-party AI platform vendors are contractually prohibited from training models on our customers' data
- Annual vendor security reviews and ongoing compliance monitoring
- Sub-processor list maintained and disclosed to LEA customers upon request

4.2 Employee Security & Training

- Background checks required for all employees with access to student data
- Annual FERPA, IDEA confidentiality, and security awareness training is mandatory
- Security training specific to SPED data handling and parent rights
- Phishing simulation and social engineering awareness programs
- Strict clean desk and device encryption policies for remote workers
- Separation of duties for sensitive data access and administration functions

4.3 Incident Response & Breach Notification

- A documented Incident Response Plan (IRP) is maintained, tested, and updated annually
- Dedicated security incident response team with defined roles and escalation procedures
- Breach notification within the timeframes required by FERPA, applicable state breach notification laws (typically 30–60 days), and contract terms
- Root cause analysis and corrective action plans documented for all security incidents
- LEA customers are notified promptly and supported through any incident affecting their data

4.4 Audit, Logging & Monitoring

- Comprehensive audit logs of all access to student data, including read, modify, export, and delete events
- Logs are tamper-evident, retained per regulatory requirements, and reviewed for anomalies
- Security Information and Event Management (SIEM) platform for real-time threat detection
- Automated alerting for anomalous access patterns, failed authentication attempts, and data exfiltration indicators
- LEA administrators can request access logs for their organization's data upon request

4.5 Data Minimization & Retention

- We collect only the student data necessary to provide contracted services (data minimization principle)
- Data retention schedules are defined in each LEA agreement and enforced programmatically
- Secure deletion (NIST SP 800-88 compliant media sanitization) upon contract termination or data deletion request
- De-identification and anonymization applied when data is used for aggregate, non-identifiable reporting

5. Frequently Asked Questions (FAQ)

We understand that LEA administrators, educators, service providers, and parents of students with disabilities have specific concerns about how student data is handled. Below are answers to the questions we hear most often.

For LEA Administrators & Leadership

Q: Does Expatriate Communications sign a Data Processing Agreement (DPA)?

A: Yes. We sign DPAs with any LEA that requires one. Our DPA template complies with FERPA, IDEA, and applicable state privacy laws. We also support the Student Data Privacy Consortium (SDPC) National Data Privacy Agreement (NDPA) framework. Contact your account representative to initiate the DPA process. We do not onboard any LEA without appropriate data governance documentation in place.

Q: Does using your AI features mean our student data is being used to train AI models?

A: Absolutely not. Our AI pipeline uses tokenization to replace all student PII with meaningless tokens before any data reaches an AI model. The AI never sees real student names, ID numbers, diagnoses, or any other identifying information. Furthermore, we contractually prohibit all AI vendors in our supply chain from using our customers' data for model training. This is a firm, non-negotiable contractual obligation in every vendor agreement we sign.

Q: How do you ensure our student data is not mixed with another LEA's data?

A: We maintain strict logical data isolation (multi-tenancy security) between all LEA customers. Each LEA's data is stored in separate, access-controlled partitions. Our access control system enforces that users can only ever access data belonging to their own LEA. This isolation is validated through regular security testing.

Q: What happens to our student data if we end our contract with Expatriate Communications?

A: Upon contract termination, you retain full rights to your data. We provide a full data export in a portable format within 30 days of termination. After you confirm receipt and acceptance of the export, we securely delete all copies of your data — including backups — per NIST SP 800-88 standards, and provide written certification of deletion upon request.

Q: Can our IT team review your security certifications and audit reports?

A: Yes. We can provide a SOC 2 Type II report summary, our most recent third-party penetration test executive summary, and our security policy documentation under a mutual NDA upon request. We welcome LEA security teams to conduct a vendor risk assessment and will respond to standard security questionnaires (SIG, CAIQ, etc.).

For Special Education Administrators & Case Managers

Q: Are SPED records (IEPs, evaluations, FBAs, BIPs) treated differently than general education records?

A: Yes. We classify SPED records as the highest sensitivity tier in our data classification framework. IDEA Part B requires stricter confidentiality protections than general FERPA requirements, and we apply those stricter standards. Access to IEPs, psychological evaluations, functional behavioral assessments, behavior intervention plans, and related services records is restricted to personnel with a documented legitimate educational interest in that specific student.

Q: How is access to a student's IEP or evaluation report controlled?

A: Access is controlled through Role-Based Access Control (RBAC). Only users whose role includes the student on their active caseload can view SPED records. A general education teacher who is not part of a student's IEP team does not have access to that student's IEP. Administrators can configure team-based access, and every access event is logged and auditable.

Q: How does the system handle Medicaid billing data for school-based services?

A: Medicaid billing data involves a FERPA/HIPAA overlap and is treated with the highest level of protection. We follow the joint U.S. Department of Education and HHS guidance on this overlap. Parental consent records for Medicaid billing are maintained separately and are never shared or repurposed beyond the billing function.

Q: What controls are in place when sharing student records with outside agencies (e.g., Part C programs, VR agencies)?

A: Inter-agency data sharing is only performed upon documented written consent from parents or eligible students, or under a valid FERPA exception (such as a court order or audit). We maintain a complete log of all data disclosures. Our system supports the generation of consent-to-release documentation and tracks disclosure history for each student record.

For Service Providers & Related Services Staff

Q: Can I access student records for all students, or only those on my caseload?

A: You can only access records for students on your active, assigned caseload. Our system enforces this through Role-Based Access Control. If a student is transferred to a different provider or removed from your caseload, your access is automatically revoked. Any attempt to access unauthorized student records is logged and will trigger a security review.

Q: Is it safe to access the platform from a personal device or a home network?

A: Our platform enforces HTTPS encryption on all connections, so your data is protected in transit regardless of the network you use. However, LEA security policies may restrict the use of personal devices for accessing student records. We strongly recommend following your LEA's Acceptable Use Policy (AUP) and using LEA-managed devices and networks whenever possible. We support integration with LEA Mobile Device Management (MDM) systems.

Q: What should I do if I accidentally see another student's information I shouldn't have access to?

A: Report it immediately to your LEA's Privacy Officer or system administrator, and also notify us at our security contact. Do not access, copy, or share the information. All accidental disclosures should be treated as potential FERPA incidents. Our security team will investigate to determine if a misconfiguration caused the exposure and will remediate immediately.

For Parents & Guardians of Students with Disabilities

Q: Who can see my child's IEP, evaluation, and other special education records?

A: Under IDEA and FERPA, only school officials and staff with a legitimate educational interest in your child may access their records. This includes your child's IEP team members, their service providers, and relevant administrators. Expatriate Communications' system enforces these restrictions

technically — access is controlled, logged, and audited. No one outside your child's educational program can access their records without your written consent or a legally permitted exception.

Q: Is my child's disability information being used by any AI system?

A: Your child's personal information — including their name, ID, diagnosis, and any other identifying details — is never sent to any AI system in a form that could identify them. Our AI pipeline uses a process called tokenization, which replaces all identifying information with meaningless codes before any AI processing occurs. The AI only ever sees those codes, not your child's real information. Your child's data is never used to train any AI model.

Q: Can my child's data be sold to anyone?

A: No. Expatriate Communications does not sell student data under any circumstances. We do not share your child's information with advertisers, data brokers, marketing companies, or any entity outside the educational services we are contracted to provide. This is both our policy and a contractual obligation with every LEA that uses our platform.

Q: How do I request to see or correct my child's records in the system?

A: Your rights to inspect, review, and request amendment of your child's educational records are guaranteed by FERPA and IDEA. To exercise these rights, contact your child's school or LEA directly — they are the official custodians of your child's educational records. Expatriate Communications supports LEAs in responding to these requests by providing the necessary tools to access and export records. LEAs are required to respond to inspection requests within 45 days under FERPA.

Q: What happens to my child's data after they leave the school district or when they turn 18?

A: Record retention is governed by FERPA, IDEA, and your state's records retention schedules. When a student transitions out of SPED services, records must be retained for a minimum period (at least until the student turns 26 under IDEA eligibility timelines in many states). Upon request, the school must notify parents (or eligible students who have assumed their own rights at age 18) before destroying records. Expatriate Communications enforces the retention schedule set by your LEA and supports secure record export and deletion workflows.


Q: What if there is a data breach that affects my child's information?

A: If a security incident occurs that may have exposed your child's information, your LEA is required to notify you in accordance with FERPA breach guidance and applicable state breach notification laws. Expatriate Communications will immediately notify the LEA of any confirmed breach, provide full details of what data was involved, and support the LEA in their notification obligations. We take responsibility for our role in any incident and are committed to transparency. Affected families will be provided with clear information about what happened, what data was involved, and what steps are being taken.

6. Contact & Accountability

Expatriate Communications maintains dedicated contacts for data security and privacy inquiries:

Contact	For
Data Privacy Officer (DPO)	FERPA/IDEA compliance questions, parent rights requests, record inspection/amendment inquiries
Security Team	Security incidents, vulnerability disclosures, penetration test results, security questionnaires
Legal & Compliance	DPA negotiations, state compliance questions, subpoenas and legal process requests
Account Representative	Vendor risk assessments, SOC 2 reports, audit support, general platform inquiries

 **Document Governance:** This policy is reviewed and updated annually, or more frequently in response to changes in applicable law, regulatory guidance, or material changes to our data handling practices. The current version is always available to LEA customers upon request.

© 2025 Expatriate Communications, Inc. | All Rights Reserved | This document is intended for LEA customers, authorized users, and parents of students served by Expatriate Communications platforms.