DATA PRIVACY AND SECURITY PLAN

Openfire LLC DBA Snack

2655 N Ocean Drive, STE 405, Singer Island, FL 33404
support@snack.io | 502-617-6225 | snack.io

Prepared pursuant to New York Education Law § 2-d and 8 NYCRR Part 121

Overview

This Data Privacy and Security Plan ("Plan") is maintained by Openfire LLC DBA Snack ("Provider") and describes the administrative, operational, and technical safeguards in place to protect personally identifiable information ("PII") received pursuant to agreements with Educational Agencies ("EA"). This Plan is provided in accordance with New York Education Law § 2-d and Section 121.6 of the Commissioner's Regulations, and aligns with the NIST Cybersecurity Framework (CSF) v1.1.

This Plan applies to all Student Data and, where applicable, APPR Data received from EAs under signed Data Privacy Agreements (DPAs). It is reviewed and updated at least annually or upon material changes to the Provider's infrastructure, personnel, or applicable legal requirements.

Section 1: Implementation of Data Security and Privacy Contract Requirements

Openfire LLC DBA Snack implements data security and privacy requirements through a combination of contractual commitments, technical controls, and ongoing operational practices maintained for the full duration of each service agreement.

Upon execution of a Data Privacy Agreement (DPA), the Provider:

- Designates a responsible point of contact for privacy and security matters reachable at support@snack.io
- Binds all employees and subprocessors with access to Student Data to the terms of the applicable DPA through written agreements
- Activates logical separation of student data from non-educational customer data within Provider systems
- Ensures all applicable subprocessors are operating under zero-data-retention agreements for AI-processed content

The Provider's published Privacy Policy (snack.io/privacy) governs data handling practices and is reviewed at minimum annually. Material changes to privacy practices are communicated to organizational customers prior to taking effect. Student Data received under any DPA is used solely to provide the contracted services and is never used for advertising, product development, or any commercial purpose.

Compliance with applicable federal and state student privacy laws -- including FERPA, COPPA, and applicable state statutes -- is treated as a baseline operational requirement enforced continuously over the life of each contract.

Section 2: Administrative, Operational, and Technical Safeguards

Administrative Safeguards

- Designated privacy and security point of contact: support@snack.io
- Written Privacy Policy and Data Security and Privacy Plan reviewed annually
- Written Data Processing Agreements (DPAs) executed with all EAs prior to data receipt
- Written subprocessor agreements prohibiting independent use of Student Data
- Annual review of data retention schedules and disposition procedures
- Background check policy for employees with direct student contact

Operational Safeguards

- Role-based access controls -- access to Student Data limited to personnel with a legitimate operational need
- Multi-factor authentication (MFA) enforced on all administrative and privileged accounts
- Employee onboarding includes training on FERPA, COPPA, and applicable state student privacy laws
- Subprocessors reviewed for privacy and security compliance prior to engagement
- Immutable audit logging for sensitive administrative operations
- Written incident response plan maintained and tested; available to EAs upon request

Technical Safeguards

- All data encrypted in transit using TLS 1.2 or higher
- All data encrypted at rest using industry-standard encryption
- Application hosted on SOC 2-compliant cloud infrastructure (US regions only)
- Student data stored in managed database infrastructure with row-level security and logical tenant isolation
- Video and media content processed through contracted third-party infrastructure operating under data processing agreements
- AI features operate under zero-data-retention agreements -- content is deleted after processing and not used for model training
- Time-limited, signed URLs for all stored media access
- Automated error monitoring with 90-day log retention; diagnostic data limited to identifiers needed for bug resolution
- Regular vulnerability assessments and security monitoring

Section 3: Employee and Subcontractor Training on PII Confidentiality

All Provider employees and agents who have access to Student Data or PII are trained on the confidentiality requirements governing that data prior to receiving access. Training covers:

- The requirements of FERPA and its implementing regulations
- The requirements of COPPA and applicable state student privacy laws (including New York Education Law § 2-d)
- The Provider's own Privacy Policy and internal data handling procedures
- Obligations under executed DPAs, including restrictions on use, redisclosure, and commercial exploitation of Student Data
- Incident identification and reporting procedures

Training is conducted at onboarding and reviewed annually or when material changes to applicable law or Provider policy occur. All employees with data access sign a written confidentiality acknowledgment as a condition of employment.

Subprocessors engaged by the Provider who will have access to Student Data are required to demonstrate appropriate training of their own personnel as a condition of their subprocessor agreements.

Section 4: Contracting Processes Binding Employees and Subprocessors

The Provider ensures that all personnel and subprocessors with access to Student Data are bound by written agreements that incorporate, at minimum, the requirements of the applicable DPA.

Employees

- All employees who may access Student Data execute a written confidentiality agreement as a condition of employment
- Access to Student Data is provisioned on a least-privilege basis and tied to specific job functions
- Employee agreements expressly incorporate the Provider's obligations under executed DPAs

Subprocessors

- All subprocessors are engaged under written Data Processing Agreements (DPAs) or equivalent contractual instruments
- Subprocessor agreements prohibit independent use of Student Data for any purpose beyond fulfilling contracted services
- Subprocessor agreements require data security practices no less stringent than those required of the Provider
- Subprocessor agreements require prompt notification to Provider of any breach or unauthorized access involving Student Data
- AI and transcription subprocessors operate under zero-data-retention agreements, deleting submitted content immediately after processing

A list of current subprocessors is available upon request by contacting support@snack.io. EAs are notified of material changes to the subprocessor list prior to such changes taking effect.

Section 5: Incident Management, Breach Identification, and EA Notification

The Provider maintains a written Incident Response Plan (IRP) that governs the identification, containment, investigation, and notification processes for any security or privacy incident involving PII. The IRP is reviewed and updated at least annually.

Breach Identification

- Automated monitoring and alerting is in place across application infrastructure to detect anomalous activity
- Error monitoring tools capture and flag unauthorized access attempts and unexpected system behavior
- Audit logs are maintained to support forensic analysis of potential incidents
- Immutable administrative audit trails enable reconstruction of data access events

Notification Obligations

- In the event of a confirmed breach involving Student Data, the Provider will notify affected EAs within seventy-two (72) hours of confirmation, unless delayed by law enforcement direction
- For Virginia EAs: initial notification within twenty-four (24) hours of reasonably expecting a breach
- Breach notifications will include: type of data involved, estimated date/date range, general description of the incident, and Provider point of contact
- Provider will cooperate with EA, NYSED Chief Privacy Officer, and law enforcement as required
- Provider will bear costs of EA notification where breach is attributable to Provider or its subprocessors

Incident Response Process

- Containment -- isolate affected systems and revoke compromised credentials immediately upon confirmation
- Assessment -- determine scope, data types involved, and affected individuals
- Notification -- notify EA within required timeframes; notify applicable regulators as required by law
- Remediation -- address root cause, implement fixes, update controls
- Post-incident review -- document lessons learned and update IRP accordingly

EAs may request a summary of the Provider's written Incident Response Plan at any time by contacting support@snack.io.

Section 6: Data Transition to the EA

Upon written request from an EA, the Provider will deliver all Student Data held under the applicable service agreement to the EA within sixty (60) days (or within the timeframe specified in the applicable DPA, whichever is sooner).

Data transfers are provided in a structured, machine-readable format (e.g., CSV or JSON export) as agreed with the EA. The Provider will work cooperatively with the EA to ensure a complete and accurate transfer of all Student Data in Provider systems.

Upon confirmation that data transition is complete and the EA has received all applicable data, the Provider will proceed with secure destruction of its copies as described in Section 7 below, unless retention is required by law or expressly authorized in the service agreement.

Section 7: Secure Destruction Practices and Certification

The Provider destroys Student Data in a manner that renders it unrecoverable, using the following practices:

- Electronic data is securely deleted using industry-standard cryptographic erasure or overwrite methods consistent with NIST SP 800-88 guidelines
- Managed database records are permanently deleted at the row and table level; deletion propagates to replicas within standard replication windows
- Cloud object storage containing Student Data (video files, documents, uploads) is permanently deleted; Provider confirms deletion through storage provider APIs
- Backup copies containing Student Data are purged within ninety (90) days of primary system deletion
- AI processing data is deleted by subprocessors immediately after processing under zero-data-retention agreements

Upon completion of data destruction, the Provider will provide written certification to the EA confirming:

- The date destruction was completed
- The categories of data destroyed
- The destruction method(s) used

Certification is provided within thirty (30) days of destruction completion. EAs may request certification at any time by contacting support@snack.io.

Section 8: Alignment with EA Applicable Policies

The Provider is committed to aligning its data security and privacy practices with the policies of each Educational Agency it serves.

- Upon execution of a DPA, the Provider reviews the EA's Data Security Policy (where provided) and ensures its practices are consistent with EA requirements
- For New York EAs: the Provider's practices align with the NYSED Data Security and Privacy Policy and incorporate the EA's Parents Bill of Rights for Data Security and Privacy as provided in Exhibit J
- The Provider's Privacy Policy (snack.io/privacy) is publicly available and updated to reflect current practices and applicable legal requirements
- The Provider will notify EAs of material changes to its privacy policy at least fifteen (15) days prior to such changes taking effect
- The Provider will provide a copy of its data privacy policy within fifteen (15) days of written request from any EA
- Upon audit request, the Provider will cooperate with the EA or its designees, including providing access to relevant records, facilities, and staff as described in the DPA

EAs with specific policy requirements not addressed in this Plan are encouraged to contact support@snack.io so the Provider can work to meet district-specific needs.

Section 9: NIST Cybersecurity Framework v1.1 Alignment

The table below describes how the Provider's data security and privacy practices align with the twenty-three (23) categories of the NIST Cybersecurity Framework v1.1. The Provider's primary framework selection is NIST CSF v1.1 as indicated in Exhibit F of the applicable DPA.

Function / Category	Description	Provider Response
IDENTIFY (ID)		
Asset Management (ID.AM)	Data, personnel, devices, systems, and facilities are identified and managed consistent with organizational objectives and risk strategy.	Provider maintains an inventory of all systems that store or process Student Data, including application infrastructure (US-based cloud hosting), managed database services, video processing infrastructure, and AI subprocessors. Data flows are documented and reviewed when infrastructure changes occur. Student data is logically isolated from non-educational customer data.
Business Environment (ID.BE)	The organization's mission, objectives, stakeholders, and activities are understood and prioritized to inform cybersecurity roles and responsibilities.	Provider is an EdTech SaaS company whose mission includes responsible stewardship of student data. Privacy and security responsibilities are assigned to the founding team, with the designated privacy contact reachable at support@snack.io. Cybersecurity considerations are incorporated into product development and vendor selection decisions.
Governance (ID.GV)	Policies, procedures, and processes to manage regulatory, legal, risk, and operational requirements are understood and inform cybersecurity risk management.	Provider maintains a published Privacy Policy (snack.io/privacy), this Data Security and Privacy Plan, and written DPAs with all EAs. Policies are reviewed at least annually. The Provider monitors changes to applicable federal and state student privacy laws (FERPA, COPPA, NY Ed Law § 2-d, and others) and updates practices accordingly.
Risk Assessment (ID.RA)	The organization understands cybersecurity risk to operations, assets, and individuals.	Provider conducts periodic risk assessments of its application infrastructure and data handling practices. Risks identified through vulnerability monitoring, error tracking, and security assessments are triaged and remediated based on severity. Student data is treated as the highest sensitivity classification.
Risk Management Strategy (ID.RM)	Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Provider's risk tolerance for Student Data incidents is minimal. Security investments are prioritized to protect PII above other data categories. Provider maintains cyber liability insurance coverage and has documented incident response procedures to manage residual risk.
Supply Chain Risk Management (ID.SC)	Processes to identify, assess, and manage supply chain risks are established and implemented.	All subprocessors with access to Student Data are evaluated for security practices prior to engagement and bound by written DPAs. AI and transcription subprocessors operate under zero-data-retention agreements. Provider maintains a current subprocessor list available upon request. EAs are notified before material subprocessor changes take effect.
PROTECT (PR)		
Identity Management, Authentication and	Access to physical and logical assets is limited to authorized users	Multi-factor authentication (MFA) is enforced on all administrative and privileged accounts.

Function / Category	Description	Provider Response
Access Control (PR.AC)	and managed consistent with assessed risk.	Role-based access controls limit Student Data access to personnel with a legitimate operational need. Time-limited, signed URLs restrict media access. Managed database infrastructure enforces row-level security and tenant isolation. Access is reviewed when personnel roles change.
Awareness and Training (PR.AT)	Personnel and partners are provided cybersecurity awareness education and trained to perform cybersecurity duties.	All employees with access to Student Data receive training on FERPA, COPPA, NY Education Law § 2-d, and Provider's internal data handling policies prior to data access. Training is repeated annually and updated when applicable laws or policies change. Employees sign written confidentiality acknowledgments. Subprocessors are required to maintain equivalent training for their own personnel.
Data Security (PR.DS)	Information and records are managed consistent with risk strategy to protect confidentiality, integrity, and availability.	All data is encrypted in transit (TLS 1.2+) and at rest. Student data is logically separated from non-educational customer data. Data retention schedules are enforced programmatically. AI processing data is deleted immediately after processing. Backup data containing Student Data is purged within 90 days of primary deletion. PCI-compliant payment processing is used; full card numbers are never stored.
Information Protection Processes and Procedures (PR.IP)	Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.	Provider maintains written security policies including this Plan, its Privacy Policy, incident response procedures, and subprocessor management processes. Policies are reviewed annually. Configuration management practices govern application deployment. Change management processes require security review for significant infrastructure changes.
Maintenance (PR.MA)	Maintenance and repairs of information system components are performed consistent with policies and procedures.	Provider's application runs on managed cloud infrastructure where underlying hardware maintenance is handled by the infrastructure provider under their respective SOC 2 compliance programs. Software dependencies are monitored for vulnerabilities and updated on a regular cadence. Security patches are applied in a timely manner based on severity.
Protective Technology (PR.PT)	Technical security solutions are managed to ensure security and resilience of systems and assets.	Technical controls include: TLS encryption in transit, encryption at rest, MFA on administrative accounts, immutable audit logging for sensitive operations, signed URL-based media access, automated error monitoring with constrained retention (90 days), and firewall and network access controls enforced at the infrastructure layer by the cloud provider.
DETECT (DE)		

Function / Category	Description	Provider Response
Anomalies and Events (DE.AE)	Anomalous activity is detected and the potential impact of events is understood.	Automated monitoring is in place across application infrastructure. Error monitoring tools capture anomalous behavior, unexpected access patterns, and system errors in real time. Audit logs enable retrospective analysis of data access events. Alerts are configured for critical security events including authentication failures and unexpected data exports.
Security Continuous Monitoring (DE.CM)	Information systems and assets are monitored to identify cybersecurity events and verify effectiveness of protective measures.	Provider conducts continuous monitoring of application health, error rates, and security events through automated tooling. Infrastructure-level monitoring is provided by the underlying cloud platform. Vulnerability scanning is performed on a regular basis. Subprocessor security posture is reviewed periodically.
Detection Processes (DE.DP)	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection procedures are documented as part of the Provider's Incident Response Plan. Alert thresholds and detection rules are reviewed when new services are introduced or after security incidents. Provider's detection capabilities are evaluated as part of periodic security assessments.
RESPOND (RS)		
Response Planning (RS.RP)	Response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents.	Provider maintains a written Incident Response Plan (IRP) covering containment, assessment, notification, remediation, and post-incident review. The IRP is reviewed and updated at least annually. Roles and responsibilities for incident response are assigned to designated personnel. EAs may request a summary of the IRP at any time.
Communications (RS.CO)	Response activities are coordinated with internal and external stakeholders.	In the event of a confirmed breach involving Student Data, Provider notifies affected EAs within 72 hours of confirmation (24 hours for Virginia EAs). Provider cooperates with EA, NYSED Chief Privacy Officer, and law enforcement as required. Internal communications follow escalation procedures defined in the IRP. Subprocessors are required to notify the Provider promptly upon discovering any incident involving Student Data.
Analysis (RS.AN)	Analysis is conducted to ensure effective response and support recovery activities.	Upon detecting a potential incident, Provider conducts analysis to determine scope, affected data categories, affected individuals, and root cause. Audit logs and error monitoring data are used to reconstruct events. Findings are documented and used to inform notification content and remediation steps.
Mitigation (RS.MI)	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Mitigation actions include: immediate isolation of affected systems, revocation of compromised credentials, blocking of

Function / Category	Description	Provider Response
		identified attack vectors, and engagement of infrastructure providers where applicable. The provider takes steps to prevent recurrence as part of post-incident remediation.
Improvements (RS.IM)	Organizational response activities are improved by incorporating lessons learned from detection/response activities.	After each security incident, Provider conducts a post-incident review to identify gaps in detection, response, or controls. Findings are incorporated into updates to the IRP, security controls, and training programs. Provider tracks open remediation items to closure.
RECOVER (RC)		
Recovery Planning (RC.RP)	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Provider's cloud infrastructure is hosted on platforms with documented disaster recovery capabilities and geographic redundancy. Provider maintains application-level recovery procedures including data restoration from backups where applicable. Recovery time objectives are defined and tested as part of infrastructure planning.
Improvements (RC.IM)	Recovery planning and processes are improved by incorporating lessons learned into future activities.	Post-incident reviews include evaluation of recovery procedures. Lessons learned are incorporated into infrastructure improvements, backup strategies, and recovery runbooks. Provider tracks recovery-related improvement items alongside other post-incident actions.
Communications (RC.CO)	Restoration activities are coordinated with internal and external parties.	Provider coordinates restoration activities with infrastructure providers, subprocessors, and affected EAs as appropriate. EAs are kept informed of restoration status and expected timelines during and after an incident. Provider engages legal counsel as needed for regulatory communications during recovery from significant incidents.

Certification

The undersigned authorized representative of Openfire LLC DBA Snack certifies that this Data Privacy and Security Plan accurately reflects the Provider's data security and privacy practices and that the Provider is committed to maintaining compliance with all applicable federal and state student privacy laws over the life of each service agreement.

Authorized Representative: Daniel G. Cruden

Name / Title: Daniel Cruden, CEO

Date: 2026-03-30

Audit trail

Details

FILE NAME	Snack_Data_Security_Privacy_Plan.docx - 3/30/26, 2:51 PM.pdf
STATUS	Signed
STATUS TIMESTAMP	2026/03/30 18:52:31 UTC

Activity

SENT	dan@snack.io **sent** a signature request to: • Daniel G. Cruden (dan@snack.io)	2026/03/30 18:51:37 UTC
SIGNED	**Signed** by Daniel G. Cruden (dan@snack.io)	2026/03/30 18:52:31 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2026/03/30 18:52:31 UTC

The email address indicated above for each signer may be associated with a Google account, and may either be the primary email address or secondary email address associated with that account.