Classroomscreen Data Security and Privacy Plan

1. About this plan

This plan describes how Classroomscreen B.V. ("Classroomscreen") protects the personally identifiable information it receives from schools. It serves as the data security and privacy plan that schools require under their data privacy agreements and under state student-privacy laws. Annex A shows how the plan meets the requirements of New York.

The plan applies to schools, school districts and other educational organizations ("schools") that use Classroomscreen under an **organization subscription** and have signed a data privacy agreement with Classroomscreen. In this plan, "Student Data" means the student data that a school provides to Classroomscreen, or that its teachers create in Classroomscreen, under such a subscription.

Classroomscreen is a web-based classroom tool. Teachers use it on a projector, interactive whiteboard or shared screen to display screens, widgets and activities. Students do not create Classroomscreen accounts or log in. Students may join teacher-led activities through a session code without entering a name, email address or student ID. The Student Data that Classroomscreen processes is limited to what teachers enter, typically students' first names, class lists, group-maker settings and uploads that may contain student work, and to the anonymous poll votes that students submit through Join. Classroomscreen does not collect or process teacher or principal performance evaluation data.

Classroomscreen's security practices are aligned with the NIST Cybersecurity Framework (CSF) version 1.1, based on Classroomscreen's own assessment, and mapped to NIST CSF 2.0 (section 13).

2. How we implement data security and privacy requirements over the life of the agreement

- **Accountability.** A designated Privacy & Security Officer is responsible for this plan, for Classroomscreen's information security policies, and for meeting the data security and privacy requirements of each agreement. Senior management approves the policies.
- **Policies.** Nine written information security policies govern the program: information security (governance and risk), access control, acceptable use and endpoints, training, data protection and retention, vendor management, secure development and operations, incident response, and backup and recovery. They are reviewed at least annually and after significant changes.
- **Agreement register.** Classroomscreen keeps a register of every school with a data privacy agreement. It records the school's contacts, its data privacy and security policies (including any parents' bill of rights), the term of the agreement, and any data return, notice or destruction steps. The register is used to meet school-specific obligations throughout the agreement and after it ends.

- **School policies.** Classroomscreen reviews the school's data privacy and security policies when an agreement is signed (see section 9).
- **Risk management.** Security risks are recorded in a security risk register and reviewed at least annually.
- **Oversight and audits.** Classroomscreen cooperates with audits and investigations as set out in the agreement. On request, it provides its policies and related procedures to the school or to competent authorities.
- **Review of this plan.** This plan is reviewed at least annually and whenever practices change materially. Classroomscreen notifies schools at least 30 days before a material change to this plan or to its handling of Student Data takes effect.

3. Administrative, operational and technical safeguards

Administrative safeguards

- Approved information security policies with defined roles and annual review.
- A security risk register with a documented risk method and a low appetite for risks to the confidentiality of student data.
- Training on federal and state confidentiality law and on security awareness before access is granted and annually afterwards (section 4).
- Written confidentiality obligations for all staff (section 5). Staff with access to production systems or customer data also provide a Dutch certificate of conduct (Verklaring Omtrent het Gedrag). No Classroomscreen employee has direct contact with students.
- Vendor assessment before onboarding and annual vendor reviews (section 5).

Operational safeguards

- **Access control.** Access is granted on a need-to-know basis, through individual accounts. Multi-factor authentication is required for all staff access to production and administrative systems. Access rights are reviewed every quarter and revoked on the day a person leaves.
- **Support access.** Support staff can access a user's content only with that user's consent, for a limited period of at most seven days, and every access is logged.
- **Change management.** Every code and infrastructure change is reviewed by a second person and deployed through an automated pipeline. Changes are reviewed before release; in an emergency, a fix may be released first and is reviewed afterwards.
- **Vulnerability management.** Dependencies are monitored continuously for known vulnerabilities. Critical vulnerabilities are fixed or mitigated within 7 days and high vulnerabilities within 30 days. Exposed systems are scanned for vulnerabilities every quarter, and an independent third party performs a security audit and penetration test every year.
- **Monitoring.** Availability, errors and security events are monitored, alerts go to a designated responder, and alert sources are reviewed weekly.
- **Endpoints.** Staff laptops must have full-disk encryption, a firewall, built-in malware protection, automatic security updates and an automatic screen lock. Each laptop is checked when first used and annually.

- **Environments.** Production data is never used in development or test environments.

Technical safeguards

- **Encryption.** All data is encrypted in transit with TLS 1.2 or higher and at rest with AES-256. Sensitive text data is additionally encrypted at the application level.
- **Data minimization.** Students have no accounts; the Join feature does not ask students for identifying information; poll votes carry no voter identifier.
- **Logging.** Personal data is kept out of logs and error reports where possible and scrubbed before error reports are sent. Security logs are kept for up to 90 days.
- **Network protection.** Traffic passes through edge security and DDoS protection.
- **Resilience.** Data is stored redundantly across multiple locations within the same country or region, with point-in-time recovery and backups (section 12).

4. Training

Every officer, employee and contractor of Classroomscreen who will have access to Student Data completes the following training **before** receiving access, and again every year:

1. **Federal law:** training on the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), provided by iKeepSafe, an external student-privacy organization.
2. **State law:** a written summary of state student-privacy law, currently New York Education Law § 2-d and 8 NYCRR Part 121, which each person reads and signs.
3. **Security awareness:** acknowledgement of the access control and acceptable use policies and a briefing by the Privacy & Security Officer.

Completion is recorded in a training log. Access is suspended if annual training is more than 30 days overdue. Classroomscreen's subprocessors are bound by contract to protect the data they receive (section 5); Classroomscreen does not train their personnel.

5. Contracts with employees and subprocessors

Employees and contractors. Everyone who works for Classroomscreen with access to customer data is bound by a written employment or contractor agreement that includes a confidentiality clause covering customer and student data. Access is granted only after the agreement is signed and the training in section 4 is completed.

Subprocessors. Classroomscreen uses two subprocessors for Student Data:

Subprocessor	**Service**	**Student Data**
Google Cloud Platform (Google Cloud EMEA Limited)	Hosting, databases, file storage and backups	Stored in the school's organization region, the United States or the European Union; the United States for US schools

Subprocessor	Service	Student Data
Cloudflare, Inc.	Network security, DDoS protection, traffic routing and content delivery	In transit, and cached temporarily (up to 1 hour) at edge locations near the requesting user

Every vendor that processes personal data is bound by a written data processing agreement before it receives data. For Student Data subprocessors, these agreements require confidentiality, appropriate security measures, notification of security incidents, and deletion of the data when the service ends. Classroomscreen assesses each vendor's security and data location before onboarding and reviews its vendors every year. If a subprocessor fails to materially comply with these requirements, Classroomscreen notifies the affected schools, removes the subprocessor's access to Student Data, and ensures that the data is retrieved or securely deleted. Classroomscreen informs its customers at least 30 days before adding a new subprocessor for Student Data.

6. Incident management and breach notification

Classroomscreen maintains a written Incident Response Plan with state-specific procedures (currently for New York). On request, Classroomscreen gives the school a summary of the plan.

- **Identification.** Breaches and unauthorized disclosures are identified through security monitoring and alerting, the weekly review of alert sources, notices from vendors, and reports from staff and customers. Staff must report suspected incidents immediately.
- **Assessment and response.** Each incident is assigned a severity and handled by defined roles: investigation and evidence preservation, containment (for example, revoking access or rotating credentials), eradication and recovery.
- **Notification.** Classroomscreen notifies the affected school of a breach or unauthorized release of Student Data within **48 hours** after it becomes known to Classroomscreen, by email to the school's privacy or security contact, followed by a phone call to that contact or, if that contact cannot be reached, to the school's main office. The notice includes, as far as known: the types of information involved; the date or estimated date of the incident and the date of discovery; a description of the incident; the estimated number of records affected; the investigation so far; whether notification was delayed for a law-enforcement investigation; and a Classroomscreen point of contact. Information that is not yet available is provided as it becomes available. A deputy arrangement ensures that notices can be sent when the Privacy & Security Officer is unavailable.
- **Cooperation.** Classroomscreen cooperates with the school, competent authorities (such as a state education department's chief privacy officer) and law enforcement in any investigation.
- **Improvement.** Lessons learned are recorded after every significant incident. The incident response process is exercised in a tabletop exercise every year.

7. Return and transition of data

At the school's written request, during the agreement or when it ends, Classroomscreen provides an export of the school's Student Data within 30 days and at no cost. Structured data (such as screens, student lists, group-maker settings and poll results) is delivered as JSON or CSV, and uploaded files in their original format, through a secure channel. At the school's direction, the export is delivered to the school or to a successor provider the school names in writing.

8. Secure destruction and certification

- **On request.** When a school asks in writing for its Student Data to be deleted, Classroomscreen deletes it from its production systems within 30 days. Backup copies and edge caches expire within a further 30 days. The whole process, including the destruction certificate, completes within 90 days.
- **At the end of the agreement.** If the agreement ends without instructions from the school, Classroomscreen asks the school in writing, after the end, and in any case no later than 90 days after it, to confirm that its Student Data may be deleted, and deletes it as described above once the school confirms. If the school has neither confirmed the deletion nor asked in writing for the data to be kept within 180 days after the end, Classroomscreen deletes the data. If the school asks for the data to be kept, Classroomscreen keeps it until the date the school states, for no longer than 12 months after the request, and then asks again. Until deletion, the school's teachers have read-only access to the data, and the school can request an export under section 7 or deletion at any time. Classroomscreen does not retain Student Data beyond the term of the agreement except to transfer it to the school or where the law requires it.
- **Certification.** After deletion, and once backups and edge caches have expired, the Privacy & Security Officer sends the school a signed certificate stating that Classroomscreen and its subprocessors no longer have the ability to access the school's Student Data. Google Cloud removes residual copies from its own infrastructure within the period set in its data processing terms (at most 180 days); these copies are not accessible to Classroomscreen. Security logs that may contain IP addresses are not deleted per school; they expire on a rolling 90-day cycle.
- **Secure deletion.** Classroomscreen deletes Student Data with the deletion functions of Google Cloud Platform. Classroomscreen has no physical storage media. Google Cloud Platform erases or destroys its decommissioned disks under its data destruction procedures.

9. Alignment with the school's policies

Classroomscreen complies with the data privacy and security policies, including any parents' bill of rights, that a school provides under its data privacy agreement.

When an agreement is signed, and when another school joins under the same terms, Classroomscreen reviews the school's policies against this plan. Classroomscreen raises any conflict with the school before it processes Student Data. The obligations that school policies typically place on providers are covered by this plan:

- use of data only for the contracted services;
- need-to-know access;
- encryption;
- no sale or commercial use;
- subcontractor obligations;
- breach notification;
- return and destruction of data.

Where a school policy requires alignment with NIST CSF 2.0, the mapping in section 13 applies.

10. Use, disclosure and storage commitments

- Student Data is used only to provide the services described in the school's data privacy agreement.
- Student Data is never sold or used for any commercial or marketing purpose. This includes advertising and using Student Data to develop, improve or market products or services. Student Data is not used in analytics or product improvement, and no aggregated or de-identified datasets are derived from it.
- Student Data is not disclosed to any other party, except to Classroomscreen's subprocessors carrying out the agreement, or where a statute or court order requires it. In that case Classroomscreen notifies the school no later than the time of disclosure, unless the law or order prohibits notice.
- Student Data is stored in the school's organization region, the United States or the European Union, together with its backups. Student Data of US schools is stored in the United States. To deliver content quickly, copies may be cached temporarily at edge locations near the requesting user. These copies expire within 1 hour. On request, Classroomscreen provides a list of the locations where Student Data is stored.
- No Classroomscreen employee has direct contact with students.

11. Summary for schools and parents

Item	**Information**
(1) Exclusive purposes	Student Data is used only to provide Classroomscreen's classroom tool to the school's teachers under the school's organization subscription: displaying and saving classroom screens, widgets, class lists, group-maker settings, polls and uploads. It is not sold or used for any commercial or marketing purpose, including developing or improving products.

Item	Information
(2) Subcontractors	Classroomscreen uses Google Cloud Platform (hosting and storage) and Cloudflare (network security and content delivery, with temporary edge caching). They are bound by written data processing agreements requiring confidentiality, security, incident notification and deletion. Classroomscreen reviews them annually and removes access if they fail to comply. Classroomscreen staff are bound by confidentiality agreements and trained on federal and state law before receiving access.
(3) Duration and end of the agreement	The agreement remains in effect for as long as Classroomscreen has access to the school's data. During the agreement or when it ends, the school can receive its data free of charge as JSON or CSV plus original files within 30 days of a request. On the school's request, Classroomscreen deletes the data within 30 days (backups and edge caches expire within a further 30 days) and certifies the deletion. Without instructions at the end of the agreement, Classroomscreen asks the school, within 90 days at the latest, to confirm the deletion, and deletes the data after 180 days if the school has neither confirmed nor asked for it to be kept. For New York districts, Annex A applies: 90 days' notice, then deletion.
(4) Challenging accuracy	Parents, students and staff raise accuracy challenges with the school. Teachers and organization administrators can correct or delete the data directly in Classroomscreen. Classroomscreen refers any request it receives to the school.
(5) Storage and protection	Student Data is stored with Google Cloud Platform in the school's organization region, the United States or the European Union, with redundant copies and backups in the same region. Student Data of US schools is stored in the United States. To deliver content quickly, copies may be cached

Item	Information
	temporarily at edge locations near the requesting user; these copies expire within 1 hour. It is protected by access controls, multi-factor authentication for staff, monitoring, vulnerability management and the other safeguards in this plan.
(6) Encryption	Data is encrypted in transit with TLS 1.2 or higher and at rest with AES-256. Sensitive text data is additionally encrypted at the application level.

12. Business continuity and recovery

Production data is stored redundantly across multiple locations within the same country or region, with point-in-time recovery and backups that expire within 30 days. Classroomscreen's recovery objectives are a maximum data loss of 24 hours and restoration of the service within 72 hours after a major failure. A documented recovery procedure covers regional outages, data corruption and accidental deletion. Schools are informed during and after restoration.

13. Alignment with the NIST Cybersecurity Framework

The table describes, for each NIST CSF v1.1 category, how Classroomscreen's practices align. The second column lists the NIST CSF 2.0 categories to which the v1.1 category's outcomes moved, according to NIST's "CSF 1.1 to 2.0 Core Transition Changes" (2024). The Oversight category (GV.OV) is new in CSF 2.0 and is covered in the Govern table below. Classroomscreen operates no data centres or physical servers; physical protection of production infrastructure is provided by Google Cloud Platform.

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
Identify: Asset Management (ID.AM)	ID.AM, GV.RR, GV.SC	Classroomscreen maintains inventories of its data, processing activities, systems and vendors, including which vendors process Student Data. Staff laptops are recorded through an endpoint check at first use and annually. Assets are prioritized by the sensitivity of the data they

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
		hold, with Student Data as the most sensitive.
Identify: Business Environment (ID.BE)	GV.OC	Classroomscreen's mission, its role as a provider to schools, its legal and contractual obligations and its critical dependencies (Google Cloud Platform and Cloudflare) are documented in the Information Security Policy. They determine security priorities and roles.
Identify: Governance (ID.GV)	GV.OC, GV.RR, GV.PO, GV.RM	Nine information security policies, approved by senior management and reviewed annually, govern the program. A designated Privacy & Security Officer is responsible for security and privacy. Legal, regulatory and contractual requirements, including each school's policies, are identified and tracked.
Identify: Risk Assessment (ID.RA)	ID.RA	Security risks are assessed for likelihood and impact on students, schools and teachers in a security risk register, reviewed annually and after significant changes. Vulnerability information comes from continuous dependency monitoring, quarterly external vulnerability scans and an annual independent penetration test.
Identify: Risk Management Strategy (ID.RM)	GV.RM, GV.RR	A documented risk method and risk appetite apply: a low appetite for risks to the confidentiality of student

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
		data. High risks must be treated or formally accepted by senior management.
Identify: Supply Chain Risk Management (ID.SC)	GV.SC, GV.OC, GV.RM, ID.RA, ID.IM	Vendors are assessed before onboarding for their data processing terms, security and data location, and reviewed annually. Only Google Cloud Platform and Cloudflare process Student Data, both under written data processing agreements. Non-compliance leads to removal of access.
Protect: Identity Management, Authentication and Access Control (PR.AC)	PR.AA, PR.IR	Access follows least privilege and need-to-know, through individual accounts with multi-factor authentication for staff. Access is granted only after training and a signed confidentiality agreement, reviewed quarterly and revoked on departure. Support access to user content requires the user's consent, is limited to seven days and is logged.
Protect: Awareness and Training (PR.AT)	PR.AT	All staff with access to Student Data are trained on FERPA, COPPA and state student-privacy law (currently New York Education Law § 2-d) before access and annually, and receive security awareness instruction. Completion is logged, and access is suspended if training is more than 30 days overdue.

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
Protect: Data Security (PR.DS)	PR.DS, ID.AM, ID.RA, PR.PS, PR.IR, DE.CM	Data is encrypted in transit (TLS 1.2 or higher) and at rest (AES-256), with additional application-level encryption for sensitive text. Student Data is minimized, stored in the school's region (apart from edge caches near the requesting user that expire within 1 hour), never used in non-production environments, and returned or destroyed under documented procedures.
Protect: Information Protection Processes and Procedures (PR.IP)	PR.PS, PR.IR, PR.DS, ID.IM, ID.AM, ID.RA, GV.RR, GV.PO, RC.RP	Every change is peer-reviewed (an emergency fix after release) and deployed through an automated pipeline. Data is backed up with redundancy and point-in-time recovery. Incident response and recovery procedures are documented. Personnel security includes confidentiality agreements and certificates of conduct. Data is destroyed under a documented procedure with certification.
Protect: Maintenance (PR.MA)	PR.PS, ID.AM	Physical maintenance is not applicable: production runs on Google Cloud Platform. Maintenance of cloud resources is performed only by authorized staff with multi-factor authentication, through the reviewed change process.
Protect: Protective Technology (PR.PT)	PR.PS, PR.IR, PR.AA, PR.DS	Security logs are kept for up to 90 days, and personal

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
		data is kept out of logs where possible and scrubbed from error reports. Network traffic is protected by edge security and DDoS mitigation. Staff laptops require disk encryption, a firewall, malware protection, automatic updates and screen lock.
Detect: Anomalies and Events (DE.AE)	DE.AE, ID.AM	Monitoring detects anomalies such as unauthorized access attempts and abuse. Alerts go to a designated responder, and events are triaged under the Incident Response Plan.
Detect: Security Continuous Monitoring (DE.CM)	DE.CM, ID.RA, PR.PS	Availability, errors and security events are monitored continuously. Dependencies are monitored for vulnerabilities, external scans run quarterly, a penetration test runs annually, and staff laptops are checked annually.
Detect: Detection Processes (DE.DP)	GV.RR, DE.AE, ID.IM	Detection roles are defined, with the Privacy & Security Officer as responder. Alert sources are reviewed weekly, and detected events are escalated into the Incident Response Plan. Detection is improved through lessons learned and the annual tabletop exercise.
Respond: Response Planning (RS.RP)	RS.MA	A written Incident Response Plan with a severity model and state-specific

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
		procedures is executed when an incident is declared.
Respond: Communications (RS.CO)	RS.CO, RS.MA, RC.CO, PR.AT	Communication roles are defined. Schools are notified within 48 hours of a breach becoming known, with the information required by the agreement and applicable law. Classroomscreen cooperates with schools, competent authorities and law enforcement. A deputy arrangement ensures that notices can be sent when the Privacy & Security Officer is unavailable.
Respond: Analysis (RS.AN)	RS.AN, RS.MA, ID.RA	Incidents are investigated to determine cause, scope, affected records and data types, with evidence preserved.
Respond: Mitigation (RS.MI)	RS.MI, ID.RA	Incidents are contained, for example by revoking access, rotating credentials or isolating systems, and the underlying vulnerabilities are remediated.
Respond: Improvements (RS.IM)	ID.IM	Lessons learned are recorded at incident closure and after the annual tabletop exercise, and are used to update the plan and procedures.
Recover: Recovery Planning (RC.RP)	RC.RP, RS.MA	A documented recovery procedure, redundant storage, point-in-time recovery and backups support a recovery point objective of 24 hours and a

NIST CSF v1.1 category	CSF 2.0	Classroomscreen response
		recovery time objective of 72 hours.
Recover: Improvements (RC.IM)	ID.IM	After every recovery, lessons learned update the recovery procedures, policies and risk register.
Recover: Communications (RC.CO)	RC.CO	Affected schools are informed during and after restoration, using the contacts in Classroomscreen's agreement register.

NIST CSF 2.0 Govern function

CSF 2.0 category	Classroomscreen response
Organizational Context (GV.OC)	Mission, stakeholders, legal and contractual requirements and critical dependencies are documented and reviewed annually.
Risk Management Strategy (GV.RM)	A documented risk method and appetite guide decisions; high risks require treatment or formal acceptance by senior management.
Roles, Responsibilities, and Authorities (GV.RR)	A designated Privacy & Security Officer is responsible for security and privacy, with defined incident roles and a deputy arrangement. Personnel security is part of hiring and offboarding.
Policy (GV.PO)	Nine written policies, approved by senior management, are reviewed at least annually and communicated to all staff.
Oversight (GV.OV)	Senior management reviews the policies, the security risk register and this plan at least annually.
Cybersecurity Supply Chain Risk Management (GV.SC)	Vendors are assessed before onboarding and reviewed annually under written data processing agreements.

Annex A. New York

A.1 Purpose

For schools in New York, this plan is Classroomscreen's Data Security and Privacy Plan under New York Education Law § 2-d and Section 121.6 of the Regulations of the Commissioner of Education (8 NYCRR Part 121). It follows the New York State Education Department's (NYSED) model plan. This annex adds the commitments that apply only in New York and shows where the plan meets each requirement.

A.2 New York commitments

- **Framework.** Classroomscreen's security practices are aligned with the NIST Cybersecurity Framework (CSF) version 1.1, based on Classroomscreen's own assessment, and mapped to NIST CSF 2.0 (section 13). NIST CSF v1.1 is the standard adopted in 8 NYCRR 121.5 and required by the New York Data Privacy Agreement. Where a district's policy requires NIST CSF 2.0, the mapping in section 13 applies.
- **Parents Bill of Rights.** This plan incorporates the district's Parents Bill of Rights for Data Privacy and Security.
- **Services.** Student Data is used only to provide the services in Exhibit A of the New York Data Privacy Agreement.
- **APPR data.** Classroomscreen does not collect or process annual professional performance review (APPR) data of teachers or principals.
- **Commercial or marketing purpose.** The prohibition in section 10 includes every commercial or marketing purpose as defined in 8 NYCRR 121.1(c).
- **Disclosure.** Student Data is not disclosed to any other party without the prior written consent of a parent or eligible student, except as permitted by 8 NYCRR 121.9(a)(5).
- **Storage.** Student Data of New York districts is stored in the United States. This is within the regions permitted by the New York Data Privacy Agreement: the United States, Canada, the European Union, the United Kingdom, Australia and New Zealand. Temporary edge caches (section 10) are located near the requesting user, which for users in New York is in the United States, and expire within 1 hour.
- **Breach notification.** The 48-hour notice in section 6 meets the 72 hours set by the New York Data Privacy Agreement. In any case, Classroomscreen notifies the district no later than seven calendar days after discovery of the breach, as 8 NYCRR 121.10(a) requires. The notice includes the information required by the agreement and 8 NYCRR 121.10(g). Classroomscreen cooperates with the district, the NYSED Chief Privacy Officer and law enforcement (8 NYCRR 121.10(c)).
- **Breach costs.** Where a breach is attributable to Classroomscreen or its subprocessors, Classroomscreen pays for or promptly reimburses the district's full cost of notifying parents, eligible students, teachers and principals (8 NYCRR 121.10(f)). Classroomscreen also bears the costs of its required cooperation.
- **End of the agreement.** Without instructions from the district, Classroomscreen gives the district 90 days' notice and then deletes the Student Data as described in section

8, instead of waiting up to 180 days for a confirmation (Exhibit G § 11 of the New York Data Privacy Agreement). A written request from the district to keep the data is an express authorization under that section.

- **NYSED Chief Privacy Officer.** On request, Classroomscreen provides its policies and related procedures to the NYSED Chief Privacy Officer and cooperates with audits as set out in the agreement.
- **Supplemental information.** Districts may use section 11 as the supplemental information to their Parents Bill of Rights required by 8 NYCRR 121.3(c).
- **Training.** The state-law training in section 4 covers New York Education Law § 2-d and 8 NYCRR Part 121 (8 NYCRR 121.6(a)(4)).

A.3 Requirements crosswalk

Requirement	Source	Plan section
Implementation of contract requirements over the life of the contract	NYSED model question 1; 8 NYCRR 121.6(a)(1)	2, 9
Administrative, operational and technical safeguards	NYSED model question 2; 8 NYCRR 121.6(a)(2), 121.9(a)(6)	3
Supplemental information to the Parents Bill of Rights	8 NYCRR 121.6(a)(3), 121.3(c)	11
Training before access on federal and state law	NYSED model question 3; 8 NYCRR 121.6(a)(4)	4
Subcontractors bound by written agreement	NYSED model question 4; 8 NYCRR 121.6(a)(5), 121.9(b)	5
Incident management and notification	NYSED model question 5; 8 NYCRR 121.6(a)(6), 121.10	6, A.2
Return and transition of data	NYSED model question 6; 8 NYCRR 121.6(a)(7), 121.3(c)(3)	7
Secure destruction and certification	NYSED model question 7; 8 NYCRR 121.6(a)(7)	8, A.2
Alignment with the district's policies	NYSED model question 8; 8 NYCRR 121.6(a)(1), 121.9(a)(2)	9, A.2

Requirement	Source	Plan section
Alignment with NIST CSF	NYSED model question 9 and Exhibit C.1; 8 NYCRR 121.5, 121.9(a)(1)	13
Need-to-know access	8 NYCRR 121.9(a)(3)	3
Use only as authorized; no unauthorized disclosure; no sale or commercial use	8 NYCRR 121.9(a)(4), (5), (8)	10, A.2
Encryption in motion and at rest	8 NYCRR 121.9(a)(7)	3, 11
Plan warranty (a): all applicable requirements	NY Data Privacy Agreement, Exhibit G § 4(a)	Whole plan, A.2
Plan warranty (b): technical safeguards and controls	Exhibit G § 4(b)	3
Plan warranty (c): Parents Bill of Rights	Exhibit G § 4(c), § 5	9, A.2
Plan warranty (d): training	Exhibit G § 4(d)	4
Plan warranty (e): subprocessors protect PII	Exhibit G § 4(e)	5
Plan warranty (f): incident management and notification	Exhibit G § 4(f)	6, A.2
Plan warranty (g): return, deletion and destruction	Exhibit G § 4(g)	7, 8, A.2