

## DATA SECURITY AND PRIVACY PLAN

**WHEREAS**, the Groton Central School District (hereinafter “School District”) and Magoosh (hereinafter “Contractor”) entered into an agreement dated 2/5/2026 (hereinafter “Agreement”) for online test preparation (hereinafter “Services”).

**WHEREAS**, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s):

Magoosh data security and privacy practices are aligned with NIST CSF 1.1, meet FERPA and applicable New York state student privacy laws, and are consistent with the School District's Data Security and Privacy Policy. Security controls include encryption of all student data at rest (AES-256) and in transit (TLS 1.3, X25519, and AES\_128\_GCM), infrastructure hosted on AWS with monitoring through AWS CloudWatch, and centralized logging through AWS CloudTrail and SolarWinds. System and data access are restricted and employ role-based controls for limiting access, and all employees receive privacy and security training with a focus on FERPA. A third-party security assessment is conducted annually, and Magoosh has documented incident response plans for data breaches/notifications and data backups/recovery. Magoosh will make adjustments to practices as necessary to ensure alignment with District-specific policies.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

Administrative: Privacy and security training for employees, incident response plans covering data breaches/notifications and data backups/continuity of business, documented security policies

Operational: Role-based controls limiting access to systems and student data, third-party security assessments, documented incident response plans

Technical: Data encryption at rest (AES-256) and in transit (TLS 1.3, X25519, and AES\_128\_GCM), AWS infrastructure leveraging security groups, access control and WAF, continuous and centralized monitoring and logging with AWS CloudTrail and CloudWatch, and SolarWinds.

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.

- ✓ a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
- ✓ b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the “Supplemental Information” appended to the Agreement.

- ✓ c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the “Supplemental Information” appended to the Agreement.

1

- ✓ d. Student data and teacher and principal data will be stored in accordance with the “Supplemental Information” appended to the Agreement.

- ✓ e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided: *Specify date of each training*

Data security and privacy training (FERPA aligned) will be completed within 30 days of this agreement date

5. Subcontractors (check one):

Contractor shall not utilize sub-contractors.

- ✓ Contractor shall utilize sub-contractors. Contractor shall manage the relationships and contracts with such sub-contractors in the following ways in order to ensure personally identifiable information is protected:

Use of role-based access controls to restrict access to student data

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: *Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized*

*disclosures, and to promptly notify the School District.*

Magoosh maintains documented procedures to identify, respond to, and manage data security and privacy incidents involving personally identifiable information. These procedures are aligned with the NIST Cybersecurity Framework v1.1 and include mechanisms for detecting potential breaches or unauthorized disclosures, assessing impact, containing incidents, and providing prompt notification to the School District in accordance with contractual and legal requirements.

7. Termination of Agreement.

a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. Within 30 days of termination of the Agreement, Contractor shall

Return all data to the School District using \_\_\_\_\_; OR  
encrypted CSV (upon request)

2

Transition all data to a successor contractor designated by the School District in writing using encrypted CSV (upon request)

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

**IN WITNESS WHEREOF**, the Contractor hereto has executed this Data Security and Privacy Plan as of 2/5/2026.

CONTRACTOR:

Evan Marks, Head of Engineering

By: Title: 

