STUDENT DATA PRIVACY POLICY & COMPLIANCE AGREEMENT

Chicago Public Schools (SOPPA, FERPA, and Illinois School Student Records Act Compliant)

1. PURPOSE AND SCOPE

This Student Data Privacy Policy ("Policy") governs the privacy, security, and integrity of Covered Data collected, managed, or accessed by Options for Youth ("Vendor") in the course of providing digital educational services, software, or platform access to Chicago Public Schools ("District" or "CPS"). This Policy is built to strictly comply with the Illinois Student Online Personal Protection Act (SOPPA), the Family Educational Rights and Privacy Act (FERPA), the Illinois School Student Records Act (ISSRA), and all other relevant state and federal data protection statutes.

2. DEFINITIONS

- **Covered Data:** Personally identifiable information (PII) or information linked to PII in any media or format that is not publicly available and is provided by a CPS student, parent, or employee to the Vendor, or gathered by the Vendor through the operation of its educational product.
- **Targeted Advertising:** Presenting advertisements to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or covered information.
- **Subprocessor:** Any third-party service provider, cloud hosting partner, or engineering contractor engaged by the Vendor who interacts with or processes CPS Covered Data.

3. PERMITTED USES OF DATA

The Vendor shall collect, store, process, and use Covered Data solely and exclusively to deliver, maintain, and improve the educational services explicitly authorized under the Master Service Agreement with CPS. The Vendor operates as a designated school official under FERPA with a legitimate educational interest in the data.

4. ABSOLUTE PROHIBITIONS

Under no circumstances shall the Vendor engage in any of the following commercial practices:

- **No Targeted Advertising:** Engaging in targeted advertising on the Vendor's platform or any other site/service when that advertising is based on Covered Data.
- **No Profiling:** Amassing a profile, student dossier, or tracking record of a student for any purpose other than the direct fulfillment of the CPS educational contract.

- **No Commercial Sale:** Selling, renting, trading, or leasing student Covered Data to any third party for any commercial purpose whatsoever.
- **No Changes to Terms:** Modifying this Privacy Policy or any contract data terms without prior explicit, written authorization from the Board of Education of the City of Chicago.

5. DATA SECURITY REQUIREMENTS

The Vendor agrees to design, implement, and maintain a comprehensive, written information security program that contains administrative, physical, and technical safeguards appropriate to the sensitivity of Covered Data. Minimum standards include:

- **Encryption:** Protecting all Covered Data using industry-standard encryption protocols (AES-256 or higher) both while at rest within databases and during transit across public networks.
- **Access Controls:** Restricting employee and developer access to Covered Data exclusively to those individuals with a documented, verified need-to-know to fulfill the educational contract.
- **Vendor Assessments:** Routinely subjecting infrastructure to third-party vulnerability scans and independent penetration testing to ensure defensive durability.

6. SECURITY INCIDENT AND BREACH NOTIFICATION

In compliance with SOPPA timeline mandates, the Vendor shall notify Chicago Public Schools immediately and no later than **forty-eight (48) hours** after discovering or suspecting any unauthorized acquisition, access, use, or disclosure of Covered Data.

The written notification must contain a comprehensive description of the incident, the categories of data exposed, the estimated number of impacted students, and the immediate mitigation steps being taken. The Vendor shall fully indemnify and hold harmless CPS for costs associated with remediation, credit monitoring, and mandatory statutory notifications.

7. SUBPROCESSOR TRANSPARENCY AND STANDARDS

The Vendor shall not disclose Covered Data to any Subprocessor unless that third party is legally bound by identical data privacy and security constraints no less restrictive than those defined in this Policy. The Vendor must maintain an up-to-date, public-facing list of all approved Subprocessors to ensure full compliance with SOPPA transparency frameworks.

8. DATA RETENTION, RETURN, AND DESTRUCTION

The Vendor shall not retain Covered Data any longer than necessary to achieve the educational purpose stipulated in the agreement. Within thirty (30) calendar days of contract expiration, termination, or a formal written request from CPS, the Vendor shall:

1. Securely transfer all original Covered Data back to the District in a mutually agreed standard format, AND
2. Permanently and irreversibly destroy all remaining copies of the Covered Data across production environment backups and logs using NIST-compliant digital shredding mechanisms.

Upon completion of data destruction, the Vendor shall issue an official, signed Certificate of Records Disposal to the CPS Department of Information and Technology.

9. PARENT AND STUDENT RIGHTS

The Vendor recognizes that parents and legal guardians maintain statutory rights under FERPA and SOPPA to inspect, review, correct, or request the deletion of their student's records. The Vendor shall promptly refer any such requests received directly from parents or students to the District within two (2) business days and shall fully cooperate with CPS staff to fulfill the inspection or correction request.

IN WITNESS WHEREOF, the Vendor executes this Student Data Privacy Policy as a legally binding commitment to Chicago Public Schools.

VENDOR NAME: _____

Authorized Representative Signature: _____

Printed Name & Title: _____

Date of Execution: _____