SCHEDULE C-1

[Signed copy of Southern Westchester BOCES Parent Bill of Rights]

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY OF SOUTHERN WESTCHESTER BOCES

In accordance with New York State Education Law Section 2-d, the Southern Westchester Board of Cooperative Educational Services ("Southern Westchester BOCES") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

(1) New York Stated Education law Section 2-d (Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assure the confidentiality of records with respect to "third parties," and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In addition, the Southern Westchester BOCES will, upon request of parents, legal guardians or eligible students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll. An eligible student is a student who has reached 18 years of age or attends a postsecondary institution.

(2) A student's personally identifiable information cannot be sold or released for any commercial purposes;

(3) Personally, identifiable information includes, but is not limited to:

i. The student's name;

ii. The name of the student's parent or other family members;

iii. The address of the student or student's family;

iv. A personal identifier, such as the student's social security number, student number, or biometric record;

v. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

vi. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

vii. Information requested by a person who the Southern Westchester BOCES reasonably believes knows the identity of the student to whom the education record relates.

(4) In accordance with FERPA, Section 2-d and Southern Westchester BOCES Policy No. 7240, Student Records: Access and Challenge, parents and legal guardians have the right to inspect and review the complete contents of their child's education record.

(5) Southern Westchester BOCES has the following safeguards in place: Encryption, firewalls and password protection, which must be in place when data is stored or transferred.

(6) New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review at the following links or can be obtained by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234:

http://www.p12.nysed.gov/irs/data_reporting.html http://data.nysed.gov/
http://www.p12.nysed.gov/irs/sirs/documentation/nyssisguide.pdf

(7) Eligible students, parents and legal guardians have the right to have complaints about possible breaches of student data addressed. Any such complaint should be submitted, in writing, to the Data Protection Officer of Southern Westchester BOCES at dpo@swboces.org or at 450 Mamaroneck Avenue, Harrison, New York 10528. Parents can direct any complaints regarding possible breaches via the electronic form on the Southern Westchester BOCES home page, under Resources, and Student Privacy. The complaint form can also be found by going to https://bit.ly/swbdatabreach. Alternatively, a written complaint may also be submitted to the Chief Privacy Officer of the New York State Education Department using the form available at http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure or writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

Supplemental Information for Agreement with

Magic School, Inc. ,
hereinafter "Third-party Contractor") The Third-party Contractor will provide the following information and Southern Westchester Board of Cooperative Educational Services ("Southern Westchester BOCES") will review and approve or require revision of this Supplemental Information until it is acceptable to Southern Westchester BOCES.

(1) The personally identifiable student data or teacher or principal data (collectively, "the Data") received by the Third-party Contractor will be used exclusively for the following purpose(s):

"The personally identifiable student data, teacher data, or principal data (collectively referred to as ""the Data"") received by the Third-party Contractor will be used exclusively for the following purposes:

Provisioning accounts

Providing support

Improving the product through anonymized and aggregated data analysis

These purposes ensure that the data is used to enhance the educational services provided by MagicSchool while maintaining the security and privacy of the data subjects."

(2) The Third-party Contractor will ensure that all subcontractors and other authorized persons or entities to whom student data or teacher or principal data will be disclosed will abide by all applicable data protection and security requirements, including those mandated by New York State and federal laws and regulations, by the following means:

"MagicSchool ensures that all subcontractors adhere to stringent data protection and security requirements to safeguard personally identifiable information (PII). Here are the key measures in place:

High Security Standards: MagicSchool only collaborates with subprocessors who meet the highest levels of security standards, including but not limited to SOC2, ISO 27001:2013, and GDPR compliance.

Training: All employees and subcontractors receive training on state, federal, and global data security policies and procedures upon joining the company and annually thereafter.

NIST Compliant Protocols: MagicSchool follows NIST compliant protocols, including encryption at rest with AES-256 and in transit via TLS.

Data Storage: Data is stored in a US AWS Datacenter via Supabase, which provides protections including ISO, SOC, and NIST compliant controls.

Third-Party Security Standards: Third-parties must maintain reasonable organizational and technical controls, including information security policies, risk assessment programs, operations security, access control, secure system development, and physical & environmental security.

Compliance & Legal: MagicSchool considers all applicable regulations and laws when evaluating suppliers and third parties who will access, store, process, or transmit MagicSchool confidential data."

(3) The Agreement with the Third-Party Contractor will be in effect fromAugust , 2024 to June 30, 2025 . Upon the expiration of the Agreement, all student data or teacher or principal data remaining in Third-party Contractor's possession will be (check those that are applicable and fill in required information):

a. __X__ Returned to Southern Westchester BOCES and/or the public or private schools or school districts or Boards of Cooperative Education Services that purchase services through the Agreement Third-party Contractor has with Southern Westchester BOCES (collectively, referred to herein as "Purchasing Schools/BOCES" and referred to individually herein as "Purchasing School/BOCES") by August 30, 2025. If requested, we reserve the right to have the data returned to us in a format that can be easily read and imported into commonly used productivity tools, not limited to Microsoft Applications. The data should also be easily readable and organized.

b. Securely delete/destroy data belonging to the Purchasing Schools/BOCES by August 30, 2025in the following manner: At a minimum, wiping drives by writing zeros to all bits as well as using other industry standard levels of data deletion.

c. _X___ Other – explain Third-party Contractor's obligation to return the student, teacher and/or principal data may be satisfied by the offering of functionality within its products that allow the Purchasing Schools/BOCES to retrieve its own data.

(4) In the event that a student's parent or guardian or an eligible student seeks to challenge the accuracy of student data pertaining to the particular student, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to the Purchasing Schools/BOCES and processed in accordance with the procedures of the Purchasing Schools/BOCES. In the event that a teacher or principal seeks to challenge the accuracy of teacher or principal data pertaining to the particular teacher or principal, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its

Agreement with Southern Westchester BOCES, the challenge will be directed to the Purchasing Schools/BOCES and processed in accordance with the procedures for challenging annual professional performance review ("APPR") data established by the Purchasing Schools/BOCES.

(5) Describe where the Data will be stored (in a manner that will protect data security) and the security protections that will be taken by the Third-party Contractor to ensure the Data will be protected (*e.g.*, offsite storage, use of cloud service provider, etc.):

MagicSchool ensures that personally identifiable student data, teacher data, and principal data (collectively referred to as "the Data") are stored securely using a US AWS Datacenter via Supabase. This cloud storage solution is protected by several security measures to ensure data security:

Encryption:

At Rest: Data is encrypted using AES-256.

In Transit: Data is encrypted using TLS.

Compliance:

The storage solution complies with ISO, SOC, and NIST standards.

MagicSchool only works with subprocessors who meet high security standards, including SOC2, ISO 27001:2013, and GDPR.

Access Controls:

Role-based access controls are implemented to ensure that only authorized personnel can access the data.

Multi-factor authentication (MFA) is enabled for privileged users.

Regular Security Audits:

MagicSchool conducts regular security audits to ensure compliance with security policies and to adapt to new threats.

Training:

All employees and subcontractors receive training on state, federal, and global data security policies and procedures upon joining the company and annually thereafter.

(6) Third-party Contractor will use the following encryption technology to protect the Data while in motion or at rest in its custody: at a minimum of TLS1.2 or higher & 2048 bit encryption for web-based data.

Company Name: Magic School, Inc

Authorized Signature:

Authorized Signer's Name & Title: Matthew Moss-Hawkins, Senior Revenue Operations Manager

Date: 09/26/2024