EXHIBIT B

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-d of the New York State Education Law ("**Education Law 2-d**"), parents and eligible students are entitled to certain protections regarding confidential student information. The School District identified below (the "**District**") is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below. Any terms not defined herein shall have the meaning set forth in Education Law 2-d or in the Screencastify Student Data Privacy Addendum to which this document is an Exhibit.

1. Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

2. A student's personally identifiable information cannot be sold or released for any commercial purposes by a third-party contractor. The district will not sell student personally identifiable information and will not release it for commercial purposes, other than directory information released by the district in accordance with district policy.

3. Parents have the right to inspect and review the complete contents of their child's education record.

4. State and federal laws protect the confidentiality of personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

5. A complete list of all student data elements collected by the State Education Department is available for public review at http://www.p12.nysed.gov/irs/sirs/

6. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the address set forth on the signature page of this Exhibit. Complaints can also be directed to the New York State Education Department by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to CPO@mail.nysed.gov.

7. The District has entered into contracts with certain third party contractors who have received Student Data, teacher data and/or principal data. These contracts will include the following: (a) The exclusive purposes(s) for which the Student Data will be used; (b) The commencement and termination dates of each such contract; (c) A description of how parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data or the teacher or principal data that is collected; and (d) The data storage and security measures undertaken for Student Data or teacher or principal data, including whether such data will be encrypted.

8. In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the address set forth on the signature page of this Exhibit.

Name of District:	Southern Westchester BOCES / Lower Hudson Regional Center
Address:	450 Mamaroneck Ave, Harrison, NY 10528
District Authorized Representative:	Anthony Ferrante
Title:	MANAGER – IT SERVICES
Signature:	Anthony Ferrante
Date:	7/11/24

EXHIBIT C

SUPPLEMENTAL INFORMATION

District and Screencastify have entered into a Student Data Privacy Addendum ("**DPA**"). The DPA supplements the Primary Agreement and together with the Primary Agreement, is collectively referred to as the "**Agreement**." All terms not defined below or in the DPA shall have the meaning set forth in Education Law 2-d.

As required by Education Law section 2-d(3)(c) and Section 121.3 of the implementing Regulations, the following is the "**Supplemental Information**" for the Agreement with Screencastify.

1. **Purpose of Use**. Screencastify will use PII solely for the purpose of providing products and services to the Customer and as explicitly authorized in its agreement with Customer.

2. **Term and Termination of Primary Agreement**: The Primary Agreement begins and ends on the following dates as specified in the Primary Agreement: _____.

3. **Challenges to Accuracy / Deletion Requests**. As provided in Screencastify's Privacy Policy, if a parent or eligible student wishes to challenge the accuracy of or delete PII that is maintained by Screencastify, that request may be processed through the procedures provided by the Customer for amendment of education records under FERPA and the Customer may notify Screencastify of such request by emailing privacy@screencastify.com.

4. **Deletion of Customer Data.** Screencastify will delete Customer's PII so that it is physically and virtually irrecoverable within sixty (60) days of LEA's termination of its services relationship with Provider, and will provide the LEA with confirmation of such deletion upon written request.

5. **Subcontractor Oversight**. Screencastify's policy is to (i) vet prospective subcontractors and service providers who may handle PII on Screencastify's behalf to ensure they have acceptable controls in place to protect PII, (ii) only share PII with subcontractors, service providers and other third parties that are contractually bound to observe equally stringent obligations to maintain data privacy and security as are required of Screencastify pursuant to this Plan and (iii) regularly review its service providers with access to PII to ensure they continue to meet the requirements of this Plan.

6. **Security Practices and Procedures**. Screencastify has implemented the following security controls intended to provide reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the PII in its custody:

    A. Screencastify has designated a privacy officer responsible for information security governance and maintains privacy policies and practices that support compliance with the Family Educational Rights and Privacy Act ("**FERPA**"), the Children's Online Privacy Protection Act ("**COPPA**") and other applicable laws.

    B. PII is hosted in Google Cloud data centers located in the United States that maintain their own rigorous industry standard certifications and compliance offerings.

    C. Screencastify will comply with its privacy policy at www.screencastify.com/legal/privacy

D. All provisions of the Customer's Parents' Bill of Rights for data privacy and security as required by New York Ed Law 2d are incorporated into this Exhibit.

E. Screencastify provides regular privacy and security awareness training, including training on applicable laws that govern the handling of PII, to its employees who will have access to PII.

F. Screencastify limits internal access to education records and PII to those individuals that are determined to have legitimate educational interests within the meaning of §2- d and FERPA; e.g., the individual needs access to the PII in order to fulfill his or her responsibilities in performing services to the Customer;

G. Screencastify uses encryption technology and other suitable means to protect the PII in Screencastify's custody, whether in motion or at rest, from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of Health and Human Services in guidance issued under P.L. 111-5, Section 13402(H)(2), or any other technology or methodology specifically authorized by applicable statute, regulation or the New York State Education Department;

H. If Screencastify becomes aware of any breach of security resulting in an unauthorized release of Customer's PII by Screencastify or its subcontractors, Screencastify will notify Customer as required by applicable law or otherwise where Screencastify deems necessary to protect the safety and security of PII.

I. Screencastify uses a minimum encryption of AES256 for all data at rest and a minimum of TLS 1.3 for all data in transit.

J. Screencastify has dedicated employee resources charged with maintaining necessary and reasonable security controls to protect student data. The company maintains a comprehensive information security policy aligned with the controls set forth in NIST CSF v. 1.1 and relies on a combination of monitoring of data systems (such as vulnerability scans and detection processes) and access controls (for example, least privilege principles) to help ensure the security of data systems.

7. **Further Amendments.** The parties acknowledge that an addendum to this Exhibit may be necessary to ensure compliance with §2-d following the promulgation of any additional regulations and/or the issuance of further guidance by the New York State Education Department subsequent to the execution of the Agreement. The parties agree to act in good faith to take such additional steps to amend this Exhibit as may be necessary at that time.