EXHIBIT 1

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 additions, 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 Impero Solutions Inc. (DBA Ativion)

_____,
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 or teacher or principal data ("the Data") received by the Third-party Contractor will be used exclusively for the following purposes:

- To provide and support the educational functionality of the StudentKeeper and ContentKeeper platforms, including classroom management, student safeguarding, and internet filtering.
- To enable real-time visibility into student digital activity to support instructional monitoring and school safety.
- To facilitate alerting, reporting, and documentation of potential safeguarding risks (e.g., self-harm, bullying, violence) in alignment with district-designated workflows and responsibilities.
- To deliver technical support and troubleshooting for customer-authorized staff, including the configuration and maintenance of platform settings and integrations.
- To enable secure syncing of rosters, user accounts, and permissions via approved integrations with SIS platforms or identity providers (e.g., Google, Microsoft, Clever).
- To support required compliance auditing, reporting, and data retention policies as directed by the educational agency or institution.
- At no time will the Data be used for marketing, advertising, or profiling purposes, and it will not be shared with unauthorized third parties. Use of the Data will remain fully aligned with the contractual obligations under FERPA, COPPA, CIPA, and applicable state privacy laws.

(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:

- 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:

- The Contractor requires all subcontractors and authorized personnel with access to protected data to execute legally binding agreements that explicitly incorporate all applicable data privacy and security obligations. This includes adherence to FERPA, COPPA, CIPA, and New York Education Law §2-d, as well as technical and administrative safeguards consistent with NIST standards.

- Furthermore, the Contractor conducts background checks on all authorized personnel with access to PII, enforces role-based access control, and requires annual data privacy and security training. Subcontractors are also obligated to notify the Contractor of any potential or actual breach within a specified timeframe to ensure timely notification to educational agencies and regulatory authorities, in accordance with applicable law.

(3) The Agreement with the Third-Party Contractor will be in effect from July 1 , 20 25 to June 30, 20 26 . 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, 20 26 . 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.

- Student data may be returned to the Purchasing School/BOCES at any time upon request. Additionally, the Purchasing School/BOCES may choose to remove the data integration entirely, at which point data destruction can be initiated per district instruction. If requested, we will provide the data in a structured, human-readable format that can be easily imported into commonly used productivity tools such as Microsoft applications. All data will be organized and formatted to ensure clarity and usability. We will honor any request to return or destroy data in advance of the August 30, 2026 date.

b. Securely delete/destroy data belonging to the Purchasing Schools/BOCES by August 30, 20 26 in 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.

- Data destruction is carried out using industry-standard practices that meet or exceed regulatory requirements. At a minimum, this includes overwriting all bits on storage media (zeroing) and applying additional NIST-aligned data sanitization methods where appropriate. These practices ensure that no personally identifiable information (PII) is recoverable after deletion.

- If requested by the Purchasing School/BOCES, data will be destroyed immediately following the return or export of any requested records. All deletions are logged for audit purposes, and confirmation of data destruction can be provided upon request.

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.):

- For ContentKeeper and StudentKeeper, which is powered by ContentKeeper, the storage location is typically the Customer's region.
    - Specifically, for US-based Customers, their data is kept within the US.

Ativion utilizes Microsoft's Azure Cloud to host elements of its websites and Services. This indicates the use of a cloud service provider for data storage.

Security Protections Taken by Ativion for the Data:

Ativion, acting as a data processor for educational agencies, implements various security measures to protect personally identifiable data, including data from ContentKeeper:

- Ativion is required to maintain appropriate technical and organisational measures to protect against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data. These measures are subject to technical progress and development and are updated or modified over time.
- These measures are designed to ensure the security, confidentiality, and integrity of Customer Data.
- The technical and organisational measures include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, and ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident.
- Ativion implements administrative, technical, and physical access controls designed to protect the security, confidentiality, and integrity of Personal Data. These controls are designed to protect against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data.
- Encryption is used in transit (TLS 1.2+) and at rest.
- Strict user access controls are in place. Access to Personal Data is limited to those personnel performing Services in accordance with the Agreement. This is based on a principle of least privilege.
- Every access or attempt to access personal data is logged and actively monitored. Staff actions within the platform are logged and auditable.
- Ativion uses industry-standard firewalls and password protection.
- Regular monitoring of compliance with security measures is performed.
- Ativion employs regular vulnerability scanning and patching as part of its secure data practices.
- Subprocessors are engaged under written agreements containing data protection obligations not less protective than those in the Data Processing Addendum.
- Ativion is committed to complying with NYS Education Law §2-d, FERPA, COPPA, CIPA, and other applicable data protection laws and regulations.
- Ativion maintains policies to demonstrate compliance with its DPA and Data

Protection Laws and Regulations. Ativion also complies with the EU General Data Protection Regulation (GDPR) where applicable, and controls required for GDPR compliance are implemented throughout its service delivery model. It also takes into account the UK's similar legislation, the Data Protection Act 2018.

- In the context of transfers outside the EEA or UK, Ativion relies where required on appropriate or suitable safeguards or specific derogations recognized under the GDPR or UK law, which may include using Standard Contractual Clauses. For transfers from the UK, an International Data Transfer Addendum may be used.
- Customer (the educational agency) retains control over vendor access via role-based permissions and can apply expiration dates. All access changes require district confirmation and are fully audited. Customers can revoke, modify, or set expiry for Ativion Support access, and these changes are logged and maintained through a centralized audit system.
- Investigations are conducted, and mitigation steps taken in the event of a data breach or unauthorized disclosure. Documentation of findings, steps taken, and resolution timelines is made available.

In summary, ContentKeeper data is stored within the Customer's geographic region (e.g., US data in the US), utilizing Microsoft Azure Cloud. Ativion employs a comprehensive set of technical, organizational, and administrative security measures, including encryption, access controls based on least privilege, logging and monitoring, regular security assessments, and compliance with relevant data protection laws and frameworks (like FERPA, NYS Ed Law 2-d, GDPR, NIST, etc.) to protect this data.

(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.

	SOUTHERN WESTCHESTER BOARD OF COOPERATIVE EDUCATIONAL SERVICES
Signed by: Steve Stolfi FC3FE6CC10F04FC...	DocuSigned by: Victor Pineiro C5E40DF8497A4F0...
Signature	Signature
Steve Stolfi	Victor Pineiro
Print Name of Signer	Print Name of Signer
Chief Commercial Officer	Dir. of Technology/DPO
	Title
02 September 2025 | 5:52 PM BST	04 September 2025 | 3:29 PM BST
Date	Date