

Finance Manager

FINANCE MANAGER

DATA SECURITY AND PRIVACY PLAN

1. **Purpose.** The purpose of this Data Security and Privacy Plan is to define Finance Manager's security and privacy practices related to processing an Educational Agency's ("Customer") Personally Identifiable Information contained in (i) Student Data and (ii) Teacher or Principal Data (collectively, "Protected Data") in compliance with the requirements of New York Education Law 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d").
2. **Definitions.** Unless otherwise specified herein, all capitalized terms will have the meaning given to them in Section 2-d.
3. **Plan.**
 - a. **General.** When processing Protected Data, Finance Manager:
 - i. Follows policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, (ii) relevant contractual requirements between Finance Manager and the Customer; and (iii) the Customer's data security and privacy policy;
 - ii. Implements commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with Section 2-d (*see* Section (b) below);
 - iii. Follows policies compliant with the Customer Parents' Bill of Rights and Parents' Bill of Rights Supplemental Information;
 - iv. Annually trains its officers and employees who have access to Protected Data on applicable federal and state laws governing confidentiality of Protected Data; and
 - v. In the event any vendors are engaged to process Protected Data, manages relationships with vendors and contracts with vendors to protect the security of Protected Data.
 - b. **Safeguards.** Finance Manager maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its possession, including the following:
 - i. Finance Manager identifies reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;
 - ii. Finance Manager regularly assesses the sufficiency of safeguards in place to address identified risks;
 - iii. Finance Manager adjusts its security program in light of business changes or new circumstances;
 - iv. Finance Manager regularly tests and monitor the effectiveness of key controls, systems, and procedures; and

- v. Finance Manager follows written policies to protect against the unauthorized access to or use of Protected Data.
 - c. **Training.** Finance Manager trains personnel with access to Protected Data on the federal and state laws governing confidentiality of such data prior to receiving access and annually thereafter.
 - d. **Vendors.** In the event that Finance Manager engages any vendor to process Protected Data, it will (i) conduct due diligence and appropriate risk assessments before first allowing the vendor to access Protected Data, (ii) perform appropriate oversight of such vendor throughout the engagement with the vendor; and (iii) require its vendors to agree to contractual terms to protect Protected Data, including by obligating the vendor to abide by all applicable data protection and security requirements for Protected Data.
4. **Data Security and Privacy Incidents.** Finance Manager will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an Incident Response Plan (IRP) for identifying and responding to incidents, breaches, and unauthorized disclosures. Finance Manager provides notice of Breaches to Educational Agencies in accordance with its Incident Response Plan and applicable laws.
5. **Return and/or Destruction of Protected Data.** Finance Manager will implement procedures for the return, transition, deletion and/or destruction of Protected Data as follows: Finance Manager deletes all Protected Data within ninety (90) days of expiration or termination of the agreement with Customer. For clarity, the Customer, and not Finance Manager, stores and maintains all production copies of Protected Data.

FINANCE MANAGER
DATA SECURITY AND PRIVACY PLAN

1. **Purpose.** The purpose of this Data Security and Privacy Plan is to define Finance Manager's security and privacy practices related to processing an Educational Agency's ("Customer") Personally Identifiable Information contained in (i) Student Data and (ii) Teacher or Principal Data (collectively, "Protected Data") in compliance with the requirements of New York Education Law 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d").
2. **Definitions.** Unless otherwise specified herein, all capitalized terms will have the meaning given to them in Section 2-d.
3. **Plan.**
 - a. **General.** When processing Protected Data, Finance Manager:
 - i. Follows policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, (ii) relevant contractual requirements between Finance Manager and the Customer; and (iii) the Customer's data security and privacy policy;
 - ii. Implements commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with Section 2-d (*see* Section (b) below);
 - iii. Follows policies compliant with the Customer Parents' Bill of Rights and Parents' Bill of Rights Supplemental Information;
 - iv. Annually trains its officers and employees who have access to Protected Data on applicable federal and state laws governing confidentiality of Protected Data; and
 - v. In the event any vendors are engaged to process Protected Data, manages relationships with vendors and contracts with vendors to protect the security of Protected Data.
 - b. **Safeguards.** Finance Manager maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its possession, including the following:
 - i. Finance Manager identifies reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;
 - ii. Finance Manager regularly assesses the sufficiency of safeguards in place to address identified risks;
 - iii. Finance Manager adjusts its security program in light of business changes or new circumstances;
 - iv. Finance Manager regularly tests and monitor the effectiveness of key controls, systems, and procedures; and

- v. Finance Manager follows written policies to protect against the unauthorized access to or use of Protected Data.
 - c. **Training.** Finance Manager trains personnel with access to Protected Data on the federal and state laws governing confidentiality of such data prior to receiving access and annually thereafter.
 - d. **Vendors.** In the event that Finance Manager engages any vendor to process Protected Data, it will (i) conduct due diligence and appropriate risk assessments before first allowing the vendor to access Protected Data, (ii) perform appropriate oversight of such vendor throughout the engagement with the vendor; and (iii) require its vendors to agree to contractual terms to protect Protected Data, including by obligating the vendor to abide by all applicable data protection and security requirements for Protected Data.
4. **Data Security and Privacy Incidents.** Finance Manager will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an Incident Response Plan (IRP) for identifying and responding to incidents, breaches, and unauthorized disclosures. Finance Manager provides notice of Breaches to Educational Agencies in accordance with its Incident Response Plan and applicable laws.
5. **Return and/or Destruction of Protected Data.** Finance Manager will implement procedures for the return, transition, deletion and/or destruction of Protected Data as follows: Finance Manager deletes all Protected Data within ninety (90) days of expiration or termination of the agreement with Customer. For clarity, the Customer, and not Finance Manager, stores and maintains all production copies of Protected Data.

DATA PROTECTION ADDENDUM

This Data Protection Addendum (“Addendum”) is made and entered into as of the date of last signature below (“July 1, 2025”), and is incorporated into and made a part of the master services agreement (“Agreement”) between MML Software Limited d/b/a Finance Manager (“Finance Manager”) and the customer identified in the Agreement (“RIC”) to provide for compliance with the requirements of New York Education Law 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”).

1. **Definitions.** Unless otherwise specified herein, all capitalized terms will have the meaning given to them in Section 2-d and any implementing Regulations of the Commissioner of Education.
2. **Finance Manager Obligations.**
 - a. When processing Student Data and Teacher or Principal Data (“Protected Data”) on behalf of Customer, Finance Manager will comply with its obligations under Section 2-d. In particular, Finance Manager will (i) use Protected Data solely to provide the services under the Agreement and as otherwise described therein; (ii) not disclose Protected Data to any third party (excluding authorized sub-contractors) without the prior written consent of the eligible student, parent, teacher, or principal (as applicable); (iii) limit internal access to Protected Data to only those employees or sub-contractors that need access to provide the services under the Agreement; and (iv) not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or knowingly permit another party to do so.
 - b. Finance Manager will promptly notify Customer of any Breach without unreasonable delay, but no more than seven (7) days after Finance Manager has confirmed or been informed of the breach or unauthorized release.
 - c. Finance Manager will comply with Customer’s data security and privacy policy as provided to Finance Manager, together with Finance Manager’s Data Privacy and Security Plan described in Section 3 herein.
3. **Customer Obligations.** Customer represents and warrants that it owns or otherwise has and will have the necessary rights and consents in and relating to any data it makes accessible to Finance Manager, including by presenting, complying with, and enforcing all appropriate disclosure, consent, and notice requirements at the point of collection of information, so that, as accessed, received, and processed by Finance Manager in accordance with the Agreement and this Addendum, the information does not and will not infringe, misappropriate, or otherwise violate any data, privacy, or any other rights of any third party. Customer shall defend, hold harmless, and indemnify Finance Manager in the event of its breach of this Section.
4. **Data Security and Privacy Plan**
 - a. **General.** When processing Protected Data, Finance Manager::

- i. Follows policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, (ii) relevant contractual requirements between Finance Manager and the Customer; and (iii) the Customer's data security and privacy policy;
 - ii. Implements commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with Section 2-d (*see* Section (b) below);
 - iii. Follows policies compliant with the Customer Parents' Bill of Rights and Parents' Bill of Rights Supplemental Information;
 - iv. Annually trains its officers and employees who have access to Protected Data on applicable federal and state laws governing confidentiality of Protected Data; and
 - v. In the event any sub-contractors are engaged to process Protected Data, manages relationships with sub-contractors and contracts with sub-contractors to protect the security of Protected Data.
- b. **Safeguards.** Finance Manager maintains reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its possession, including the following:
 - i. Finance Manager identifies reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;
 - ii. Finance Manager regularly assesses the sufficiency of safeguards in place to address identified risks;
 - iii. Finance Manager adjusts its security program in light of business changes or new circumstances;
 - iv. Finance Manager regularly tests and monitor the effectiveness of key controls, systems, and procedures; and
 - v. Finance Manager follows written policies to protect against the unauthorized access to or use of Protected Data.
- c. **Training.** Finance Manager trains personnel with access to Protected Data on the federal and state laws governing confidentiality of such data prior to receiving access and annually thereafter.
- d. **Vendors.** In the event that Finance Manager engages any vendor to process Protected Data, it will (i) conduct due diligence and appropriate risk assessments before first allowing the vendor to access Protected Data, (ii) perform appropriate oversight of such vendor throughout the engagement with the vendor; and (iii) require its vendors to agree to contractual terms to protect Protected Data, including by obligating the vendor to abide by all applicable data protection and security requirements for Protected Data.

- e. **Data Security and Privacy Incidents.** Finance Manager will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an Incident Response Plan (IRP) for identifying and responding to incidents, breaches, and unauthorized disclosures. Finance Manager provides notice of Breaches to Educational Agencies in accordance with its Incident Response Plan and applicable laws.
 - f. **Return and/or Destruction of Protected Data.** Finance Manager will implement procedures for the return, transition, deletion and/or destruction of Protected Data as follows: Finance Manager deletes all Protected Data within ninety (90) days of expiration or termination of the agreement with Customer. For clarity, the Customer, and not Finance Manager, stores and maintains all production copies of Protected Data.
5. **Conflict.** To the extent that any terms contained within the Agreement, or any terms contained within any schedules attached to and made a part of the Agreement, conflict with the terms of this Addendum, the terms of this Addendum will apply and be given effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Effective Date.



MME SOFTWARE LTD D/B/A FINANCE MANAGER

Mercedes I Burgos
Print Name

President
Title

April 4, 2025
Date:



CUSTOMER

Tamara Reiker
Print Name

Manager Admin Apps
Title

4.9.25
Date

ATTACHMENT A
Parent's Bill of Rights for Data Security and Privacy

ATTACHMENT
EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Company is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between Sample BOCES and Company to the contrary, Company agrees as follows:

Company will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Company uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Company shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Company shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Company shall have in place sufficient internal controls to ensure that The BOCES' and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by The BOCES and/or a Participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of The BOCES and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of The BOCES and/or its Participants relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §3012-c.

Company and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law §2-d. As applicable, Company agrees to comply with The BOCES' policy(ies) on data security and privacy. Company shall promptly reimburse The BOCES and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Company, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Company shall return all of The BOCES' and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Company and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of The BOCES' and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of The BOCES' Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Company's possession and use of Protected Data pursuant to this Agreement.
2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Company's policy on data security and privacy.
3. An outline of the measures taken by Company to secure Protected Data and to limit access to such data to authorized staff.
4. An outline of how Company will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.
5. An outline of how Company will ensure that any subcontractors, persons or entities with which Company will share Protected Data, if any, will abide by the requirements of Company's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

Data Security and Privacy Plan

Version 1.0

Table of Contents

Table of Contents.....2

1.0 Purpose.....3

2.0 Terminology.....3

3.0 Relevant Laws, Regulation, Policies and Standards.....4

 3.1 Family Education Rights and Privacy Act (FERPA).....4

 3.2 New York Education Law § 3012-c(10)4

 3.3 New York State Education Law § 2-d4

4.0 Privacy, Confidentiality and Internal Controls.....5

5.0 Incident Response Plan.....6

6.0 Subcontractors6

1.0 Purpose

The purpose of this Data Security and Privacy Plan is to document **COMPANY/VENDOR'S NAME** commitment and approach to protecting Confidential Information (as defined in Section 2.0 of this plan), and how it will handle any incidents where there is a breach or unintended disclosure of Confidential Information or a System (as defined in Section 2.0 of this plan) that supports it.

2.0 Terminology

Application – means **COMPANY/VENDOR'S NAME** software that performs a user-facing function, such as a web application.

Confidential Information or Data – means any personally identifiable information related to students, student families/guardians, local education agency (LEA) employees, agents and/or volunteers obtained by or furnished to the Vendor; all findings, analysis, data, reports or other information learned or developed and based thereon, whether in oral, written, graphic, or machine-readable form; and all information marked "confidential" by the LEA. Confidential Information includes, but is not limited to, names, addresses, contact information, school or school attended, school district, grades or other reviews, credits, scores, analysis or evaluations, records, correspondence, activities or associations, financial information, social security numbers or other identifying numbers or codes, date of birth or age, gender, religion, sexual preference, national origin, socio-economic status (including free/reduced lunch status), race, ethnicity, special education status, or English Language Learner status, and any other information that constitutes "personally identifiable information" as defined in or pursuant to the Family Educational Rights and Privacy Act (20 U.S.C. 1232g and 34 C.F.R. Part 99) (collectively, "FERPA"), or "personally identifying information" as defined or used in New York Education Law 3012-c.

Confidential Information does not include any information that is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Vendor, (ii) demonstrated to have been known to the Vendor prior to disclosure by or through the LEA, (iii) disclosed with the prior written approval of the LEA, (iv) demonstrated to have been independently developed by the Vendor without reference to the Confidential Information, (v) disclosed to the Vendor by a third party under conditions permitting such disclosure, and/or (vi) disclosed as required by court order, subpoena, other validly issued administrative or judicial notice or order and/or as a matter of applicable law; provided, however, that in the event disclosure is required of the Vendor under the provision of any law or court order, the Vendor will (a) promptly notify the LEA of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the LEA to seek a protective order, and (b) disclose such Confidential Information only to the extent allowed under a protective order, if any, or necessary to comply with the law or court order; Notwithstanding the previous sentence, "personally identifiable information" as defined or used in FERPA or New York Education Law Section 2d, or "personally identifying information" as defined or used in New York Education Law §3012-c remains Confidential Information notwithstanding (A) the applicability of items (i), (ii), (iii) and (vi) in the previous sentence, and (B) items (iv) and (v) of the previous sentence to the extent that such disclosures were made at the direction of or such information was maintained on behalf of the LEA.

FERPA – means the Family and Educational Rights and Privacy Act (20 U.S.C. 1232g) and

any applicable regulations promulgated thereunder, including but not limited to 34 C.F.R. Part 99.

Handle -means (in the context of Confidential Information) to create, view, modify, store, transmit or delete.

Local Education Agency (LEA) – means a school district or an educational service agency (e.g. BOCES, RIC).

PII – means personally identifiable information, as defined under FERPA.

System - means any information technology processing device, including routers, servers, Applications, workstations and mobile devices.

Vendor – means **COMPANY/VENDOR'S NAME**, also known as **COMPANY/VENDOR'S NAME** or **COMPANY/VENDOR'S NAME**.

3.0 Relevant Laws, Regulation, Policies and Standards

3.1 Family Education Rights and Privacy Act (FERPA)

FERPA is the primary federal legislation that governs the privacy of educational records. The Vendor must hold all PII obtained, learned or developed by the Vendor in confidence pursuant to applicable provisions of FERPA. The Vendor understands that the release of PII to persons or agencies not authorized to receive such information is a violation of US federal law. Vendor understands that under FERPA it must limit access to PII to those who need to know the Confidential Information for Vendor to perform its duties under its contract, and to destroy all copies of PII, or to return PII to the LEA, when no longer needed or at the expiration of any contract. Vendor understands that upon request, it must permit the LEA access to PII that it holds, in order for the LEA to meet other obligations under FERPA or pursuant to law.

3.2 New York Education Law § 3012-c(10)

New York Education Law § 3012-c(10) governs the confidentiality of certain Confidential Information concerning teacher and principal evaluation data. Vendor understands that to the extent that information protected under New York State Education Law §3012-c(10) is shared with Vendor. Vendor is responsible for complying with this law. Vendor further understands that New York State Education Law § 2-d imposes additional requirements concerning such Confidential Information.

3.3 New York State Education Law § 2-d

New York State Education Law §2-d is a state law that imposes a number of confidentiality and data security requirements in addition to those found in FERPA and New York Education Law §3012-c(10), including a number of requirements and obligations that apply directly to Vendor. Vendor understands that it is required to comply with the requirements of New York Education Law 2-d and any regulations promulgated thereunder. Vendor understands that among other requirements, New York Education Law §2-d requires Vendor to:

- Limit internal access to Confidential Information covered under Education Law §2-d ("Covered Confidential Information") to those with legitimate educational interests;
- Not use Covered Confidential Information for any other purposes than those authorized in any contract it is party to;
- Not disclose Covered Confidential Information without parental consent, except to authorized representatives of the Vendor who are carrying out any contract it is party to;
- Maintain reasonable technical, administrative and physical safeguards to protect Covered Confidential Information;
- Not sell covered Confidential Information, nor use Covered Confidential Information for marketing purposes;
- Provide training on laws governing confidentiality to its officers, employees and assignees with access to Covered Confidential Information;
- Use encryption technology to protect Covered Confidential Information while in motion or in its custody from unauthorized disclosure, using a technology or methodology specified under HIPAA by the US Department of Health and Human Services; and
- Notify the LEA of any security breach resulting in an unauthorized release of Covered Confidential Information, and to promptly reimburse LEA for the full notification cost.

Vendor also agrees to cooperate with the LEA in complying with any regulations implementing New York Education Law § 2-d and any LEA or state policies promulgated pursuant to New York Education Law § 2-d, including but not limited to any requirements concerning (a) the inclusion of a data security and privacy plan in Vendor's contract with the LEA, (b) its compliance with any future LEA data privacy/security policy, (c) its compliance with and signature of the Parent Bill of Rights required of the LEA, and (d) the inclusion of supplemental information concerning Vendor's contract in the Parent Bill of Rights.

4.1 0 Privacy, Confidentiality and Internal Controls

COMPANY/VENDOR'S NAME will:

- A. Comply with all of the laws, regulation, policies and standards listed in Section 3.0 of this Data Security and Privacy Plan;
- B. Hold Confidential Information in strict confidence, limit internal access to it to those individuals who have a legitimate educational interest in such records (via administrative processes and Application and System authentication mechanisms), and not disclose it to any third parties nor make use of such Data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon with the LEA;
- C. Provide training on federal and state law governing Confidential Information to any officers, employees, or assignees prior to them having access to Confidential Information;
- D. Use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System, that will involve at least the following best

practice technology approaches:

- i. Authentication (i.e., passwords);
 - ii. Encryption;
 - iii. Firewalls – hardware and software;
- E. Protect and secure all Confidential Information in transit (collected, copied, and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer,
 - F. Maintain all copies or reproductions of Confidential Information with the same security it maintains the originals, and at the point in which the Confidential Information is no longer useful for its primary or retention purposes, as specified by the LEA, will destroy such Data, making it unusable and unrecoverable; and
 - G. Ensure Confidential Information will not appear in URLs of any Application.

5.1 Incident Response Plan

In the unlikely event an incident occurs where there is a breach or unintended disclosure of Confidential Information or a System that supports it, **COMPANY/VENDOR'S NAME** will adhere to this Incident Response Plan.

- A. **COMPANY/VENDOR'S NAME** will comply with all applicable breach notification laws, including New York State Education Law § 2-d and the New York State Data Breach Notification Act (General Business Law §899-aa and New York State Technology Law § 208, as appropriate).
- B. **COMPANY/VENDOR'S NAME** will notify the LEA in writing within 24 hours of the earliest indication or report of a breach or unintended disclosure of Confidential Information or a System that supports it.
- C. Response actions to incidents that might affect Confidential Information or Systems will be conducted quickly and with ample resources. **COMPANY/VENDOR'S NAME** will hire a professional third-party incident response team if in-house resources do not have sufficient skill or availability.
- D. **COMPANY/VENDOR'S NAME** will provide the LEA with the opportunity to view all incident response evidence, reports, communications and related materials, if they so request.
- E. If requested by the LEA, or if required by law, **COMPANY/VENDOR'S NAME** will notify in writing all persons affected by the incident, at its own cost and expense.

6.0 Subcontractors

In the event that **COMPANY/VENDOR'S NAME** utilizes subcontractors to support a System that Handles Confidential Information (each a "subcontractor"), such subcontractors are subject to, and **COMPANY/VENDOR'S NAME** contractually requires that each subcontractor complies with, the requirements set forth herein.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, The BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;
2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data.
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract.
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody.
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d.
7. Notify the BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without

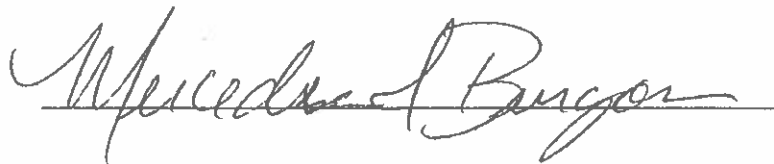
unreasonable delay.

8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract.
9. Provide a signed copy of this Bill of Rights to The BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Vendor hereby acknowledges that it is aware of and agrees to abide by the terms of this Bill of Rights. A copy of this signed document must be made a part of Vendor's Data Security and Privacy Plan.

SIGNATURE:

A handwritten signature in black ink, appearing to read "Mercedes I Burgos", written over a horizontal line.

PRINTED NAME: Mercedes I Burgos

TITLE: President

COMPANY NAME: Finance Manager

DATE: April 4, 2025

IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

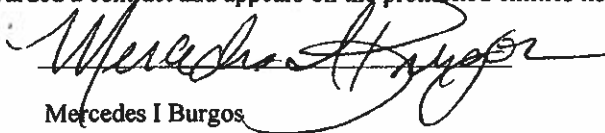
By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

Signature:



Print Name:

Mercedes I Burgos

Title:

President

Company Name:

Finance Manager

Date:

April 4, 2025

THE SAMPLE BOCES
Parents Bill of Rights - Data Privacy & Security

The School District is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with Education Law § 2-d, the District wishes to inform the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and 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.
4. A complete list of all student data elements collected by the State will be available for public review at a later date.
5. Parents have the right to have complaints about possible breaches of student data addressed. More information about where to address those complaints will be provided at a later date.

Signature:



Print Name:

Mercedes I Burgos

Title:

President

Company Name: Finance Manager

Date:

April 4, 2025

SOFTWARE LICENSING AND SUPPORT AGREEMENT

IT IS AGREED by and between MML Software LTD d/b/a Finance Manager ("FM"), with offices at 45 Research Way, Suite 207, East Setauket, NY 11733 and the Genesee Valley-Wayne Finger Lakes Educational Technology Center of Wayne Finger Lakes BOCES with offices at 131 Drumlin Court, Newark, NY 14513 ("Regional Information Center" or "RIC") effective July 1, 2025, as follows:

1. LICENSE

FM grants to RIC and to schools ("the Schools") identified by the RIC, a perpetual, non-exclusive license to use the most recent versions of certain software products as outlined in the most current FM pricing schedule ("the software"). FM shall also provide the RIC and the Schools with any upgrades and new releases of the software which become available during the term of this agreement. Use of the licensed software is limited to the RIC and the Schools and may not be sublicensed or otherwise made available to other third parties. The RIC and the Schools do not acquire any rights of ownership in the software other than a perpetual, non-exclusive license.

One copy of all modules of the software and annual maintenance will be provided at no cost to the RIC. This software will be used for Regional Information Center operations and not to account for the transactions of any specific school district or the RIC. A backup copy may also be installed for archival purposes.

FM agrees it will not consummate sales with school districts within the area served by the Regional Information Center except through the RIC. In the event that one of these entities contacts the vendor directly, FM will direct the interested party to the RIC and additionally notify the RIC of the interest and intent to purchase. However, upon consultation with and agreement by the RIC, a district of the Regional Information Center service area may purchase Finance Manager directly from Finance Manager. If the RIC ceases to designate FM as a supported software product and standard, this clause is null and void.

2. INSTALLATION, TRAINING, DATA CONVERSION & SUPPORT

FM shall provide sufficient training, training materials and documentation to the RIC staff to enable such staff to operate and use the software. Training shall be arranged at mutually agreed dates and times. FM shall provide telephone support services to resolve problems with the use of the software from 8:30 A.M. to 4:30 P.M. (Prevailing Eastern Time), Monday through Friday (excluding national holidays).

The RIC personnel assumes responsibility for all initial implementation, data conversion, processing, training, coordination, hardware consultation, hardware support (where applicable), onsite support, troubleshooting, distribution and installation of all software updates provided by FM to the schools. The RIC may subcontract any of the aforementioned services from FM in accordance with the current fees outlined in SCHEDULE A of this agreement.

3. INTELLECTUAL PROPERTY

The software, including related manuals, is owned by FM and is protected by United States copyright laws and international treaty provisions. Therefore, the RIC and the Schools agree to treat the software like any other copyrighted material, except that the RIC may make one copy of the software solely for backup or archival purposes. The RIC and the Schools further agree not to cause or permit the reverse engineering, disassembly, copying, or decomposition of the software, under the penalty of license termination, but not exclusive of other remedies. The RIC and the Schools agree not to remove any product identification, copyright notices, or other proprietary restrictions from the software or its media.

FM represents that it has the right to grant a license to the RIC and the Schools for the use of the software. If a claim is made that the use of the software infringes on or violates the intellectual property rights of a third party, FM will indemnify, defend and hold the RIC and the Schools harmless against damages, judgments and costs and expenses including but not limited to reasonable attorneys fees arising out of or in connection with the use of the software, provided that RIC and the Schools give FM timely written notice of the claim.

4. LIMITED WARRANTY AND LIABILITY

FM expressly warrants that the software will operate and perform the functions as represented by FM and that the components of the software are free from defects in material and workmanship. FM's entire liability and the RIC's and the School's exclusive remedy shall be, at FM's option, either (a) return of the price paid, or (b) repair or replacement of the software or media. THE WARRANTIES DESCRIBED ABOVE ARE IN LIEU OF ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR PURPOSE OR OTHER WARRANTIES, EXPRESS OR IMPLIED. FM does not accept liability for any loss or damage, direct, consequential or otherwise, arising out of the use of or the inability to use the software.

SOFTWARE LICENSING AND SUPPORT AGREEMENT

Page 3

5. LICENSE FEES

The RIC shall pay to FM the product license and maintenance fees (the "Fees") set out in the current FM pricing schedule in effect at the time of product installation. The RIC shall receive a ten percent (10%) discount off the list R.I.C. price of the Fees for any of the Schools that participate in an FM-related RIC service and obtain level one Support from the RIC after the effective date of this Amendment for the products and services listed in the current FM Pricing Schedule with the exception of the Timepiece and Optigate products and related fees as presented in Schedule A.

For any new Schools that purchase the Software and participate in an FM-related RIC Central Business Office or Centralized Server Service ("the Shared Server"), the product license fees shall be discounted by twenty-five percent (25%) from the list R.I.C. price outlined in the current FM pricing schedule in effect at the time of product installation. The aforementioned ten percent (10%) discount shall not apply to any of the Fees for any of the Schools that participate in the Shared Server. In addition, should any of the Schools that licensed any of the above listed products for the Shared Server wish to license these products at a later time for use on their own client/server network environment or any other third party network environment, they shall be required to pay the difference between the Fees originally paid and the Fees outlined in the current FM pricing schedule in effect at the time the transfer of software license is to commence.

Maintenance fees are subject to annual increases for any School that has purchased the Software (Not to exceed 5% in any one Year).

The Fees are payable within thirty (30) days of the later of (i) the date that the Software is installed and becomes operational, and (ii) the date of submission of an invoice.

The Fees for major upgrades to the Software will be negotiated between the parties. Major software upgrades include mandatory, Microsoft SQL Server software upgrades and platform modifications.

The Fees for new modules will be added to the current FM Pricing Schedule and become part of this agreement upon written acceptance by the RIC.

6. SOURCE CODE ESCROW

FM agrees that the source code for the software, including all updates, will be held in escrow for the benefit of, and to be provided to, the RIC in the event (a) FM files a bankruptcy petition or files a petition to convert a Chapter 11 filing to a Chapter 7 filing; (b) FM ceases to do business or (c) there is a material breach by FM to comply with its installation, training, data conversion, maintenance and support obligations under this Agreement that materially and adversely affects the material operations of the software, which breach continues for a period of more than sixty (60) days after FM has received written notice of said breach from the RIC.

FM names GUARD-IT CORPORATION having a principal place of business at 1250 S Capital of Texas Hwy, Building 3, Ste 400, Austin, Texas 78746 as the escrow agent.

SOFTWARE LICENSING AND SUPPORT AGREEMENT

Page 4

7. NOTICE

All notices, requests or demands made or given in connection with this agreement shall be in writing and given by personal delivery, certified mail or facsimile transmission to the other party at the address indicated above.

8. TERM

This agreement shall continue for one (1) year from the effective date. Fees for new licenses and annual support fees will be negotiated, in good faith, by the RIC and FM prior to the end of the term or any renewal term of this agreement.

9. GENERAL

A. This agreement contains the entire understanding and agreement between the parties. Amendments and modifications to this agreement must be in writing and signed by the party to be charged in order to be effective.

B. If any term or provision of this agreement is or becomes unenforceable, it will be severed from this agreement and the remaining terms and provisions will remain in full force and effect.

C. No term or provision of this agreement shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party granting the waiver or consent. Any such waiver or consent shall not constitute a waiver or consent to any future breach of that term.

D. This agreement shall be governed and interpreted in accordance with the laws of the State of New York.

E. This agreement shall be binding upon and inure to the benefit of the successors and assigns of each of the respective parties.

F. This agreement shall be deemed executory only to the extent of monies appropriated and available to the RIC and/or its clients for the purpose of this Agreement and no liability on account thereof shall be incurred by the RIC or its clients beyond the amount of such monies. The Agreement is not a general obligation of the RIC or its clients. Neither the full faith credit nor the taxing power of the RIC or its clients are pledged to the payment of any amount due or to become due under this Agreement. It is understood that neither this Agreement nor any representation by any public employee or officer creates any legal or moral obligation to appropriate or to make monies available from the purpose of this Agreement.

SOFTWARE LICENSING AND SUPPORT AGREEMENT

Page 5

IN WITNESS WHEREOF the authorized representatives of each of the respective parties have executed this agreement.


Date: April 4, 2025

MML Software, LTD d/b/a/ Finance Manager

By

Name: Mercedes I Burgos

Title: President

Signature: 

Date April 9, 2025

The BOCES Regional Information Center

By

Name Tamara Feiker

Title Manager Admin Apps

Signature Tamara Feiker

SCHEDULE A