SCHEDULE B

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 MML Software LTD d/b/a Finance Manager (the "Contractor") 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 the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor 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 Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor 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. Contractor 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, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time 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 ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts 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 and 3012-d.

Contractor 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, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information 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 permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

MML SOFTWARE LTD d/b/a FINANCE MANAGER

BY: Ronald J. Borch DATED: May 5, 2021

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

FINANCE MANAGER DATA PRIVACY AND SECURITY PLAN

OVERVIEW

Finance Manager provides financial and administrative software solutions to school districts and municipalities in the state of New York. Based on region, we offer software licensing and support services in one of two ways: (i) Through an authorized Board of Cooperative Educational Services ("BOCES") Regional Information Center ("RIC") and/or Central Business Office ("CBO"); (ii) Directly with the school district or municipality. Finance Manager's software is provided as a client server-based system which can be hosted either by the school district or by a BOCES RIC or CBO. Finance Manager does not host data for any clients.

As part of the Common Core Implementation Reform Act, Education Law §2-d, Section C "Parents' Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information" Finance Manager has enclosed a copy of our "Data Privacy and Security Plan". We have also outlined our response as it pertains to the handling of teacher and or principal APPR data required by school districts and BOCES hereafter:

GENERAL

Physical Safeguards

Finance Manager's offices are patrolled by security personnel. Our offices are equipped with access control mechanisms and alarm systems. During normal business hours our staff has been trained on data handling protocols as outlined in our Data Privacy and Security Plan.

SECTION 1

Q: "The exclusive purposes for which the student data, or teacher or principal data, will be used"

A: Access to "student data, or teacher or principal data" is limited to only staff members who would need access to such data for the following reasons:

1) To provide requested software application support to a school district, RIC or CBO which may potentially grant temporary access to the aforementioned data.
2) When extracting data from a third-party database for the purpose of converting a newly contracted school district's data into our software system.
3) Upgrading an existing school district from a previous version of our software which would require a change of database platform.
4) To assist when requested with the uploading of data into a school district's database for the purpose of storing current year or prior year staff ratings as required by New York State Education Department.

Finance Manager's products are used by school districts and BOCES to achieve efficient and effective operations and the licensed products are only effective with the use of school data, including PII.

SECTION 2

Q: "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"

A: Finance Manager does not share client data with any third-party contractors. It is at the sole discretion of each client to provide said data to a third party without involvement from our staff.

If a school district submits a formal request for a data extract to be created by Finance Manager for the purpose of providing said data to a third party, we would create a file extract routine which could be run within the school district's network environment. It is then at the client's discretion to provide the extracted data to the third party without the involvement of Finance Manager staff and should comply with the entity's Data Security and Privacy Plan.

SECTION 3

Q: "When the agreement with the third-party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement"

A: In the event that data needs to be held in our secured data environment for a temporary period of time for any of the purposes outline in SECTION 1 above and our agreement with that client has expired, the data shall be deleted in its entirety within 90 days from the expiration of the agreement.

SECTION 4

Q: "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"

A: Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

SECTION 5

Q: "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."

A: Any client data that has been securely transmitted to Finance Manager premises shall be stored in encrypted volumes and protected behind our firewall within the United States. Access to said data is limited to only staff member(s) for the purposes outline in SECTION 1 above. In the event that our agreement with a client has expired, said data shall be deleted in its entirety within 90 days from the expiration of the agreement. Finance Manager also uses Absolute Computrace as an added layer of protection in case of accidental loss or theft of devices such as laptops, tablets, workstations, etc. Computrace allows for remote tracking (geolocation), remote wipe, device freeze with message to user and theft recovery. Computrace is persistent and embedded into the device firmware. Even if the agent is unloaded the persistence module will reinstall the agent automatically.

In the event of a breach of data, Finance Manager shall immediately notify BOCES and advise it as to the nature of the breach and any steps we have taken to minimize said breach. Finance Manager employees are required to immediately notify a senior staff member of any breach of data to ensure rapid response to any breach which may occur while handling sensitive client data.

FINANCE MANAGER DATA PRIVACY AND SECURITY PLAN INTERNAL GUIDELINES

1.0 Purpose

Every Finance Manager employee must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our contracted clients. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical.

It is not anticipated that this technology control can effectively deal with a malicious theft scenario. Its primary objective is user awareness and avoidance of accidental loss. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale for such policies. Finance Manager and its employees are expected to practice sound judgement when handling client data which should be considered sensitive and confidential.

Finance Manager employees have been trained and must adhere to this policy regarding safe handling and protection of client data. Failure to do so could result in, but is not limited to, termination, litigation, fines, etc.

Finance Manager employees are expected to report to an officer of the company any malfeasance/malice/mishandling with regard to client data. All visitors must be escorted by an authorized employee at all times and should be restricted to appropriate areas only. If an unknown, unescorted or unauthorized person(s) is seen on Finance Manager premises, employees must notify an officer of the company immediately. Terminated employees are required to return all records, in any format, containing company or client information.

2.0 Scope

A "client" is defined as an entity under contract with Finance Manager directly or through BOCES. This could include, but is not limited to, school districts, BOCES/RICs and CBOs. Sensitive client data ("data") is defined but not limited to information relating to personnel, financial, banking, personally identifiable information ("PII") such as SSN, DOB, names, addresses, and bank account numbers, Family Educational Rights and Privacy Act ("FERPA"), etc. or any items designated as Financial, Restricted/Sensitive, Confidential or Intellectual Property.

3.0 Policies

Password/Passcode Protection Policy

All employees of Finance Manager are assigned a door passcode and are obligated to never divulge that number to anyone who is not an officer of the company. Also, it is expected that all employees protect their domain password in this same manner. In the event that an employee's password needs to be changed/reset, a default password will be assigned and the employee is required to change the password upon next successful login. Password protection goes beyond the Finance Manager internal domain. Any outside services where a password is used should be kept protected. Written lists of passwords, sticky notes, etc. are not acceptable and could be considered a violation of the password protection policy.

3.0 Policies - Continued

Remote Troubleshooting/Support Policy

Finance Manager has a GoToAssist first policy where all remote troubleshooting and support cases should attempt to use GoToAssist before using a fallback tool like RDP, etc. GoToAssist allows protections to the company and client in instances where there may be questions about the work or steps performed to resolve a case.

File and Data Transfer Policy

All attempts to remotely troubleshoot and solve support cases must be exhausted before considering transmission of client data to our site. The preferred method of transferring data to Finance Manager is through the use of Sharefile. If a client does not allow online access to our Sharefile account, other acceptable means include VPN (Virtual Private Network), RDP (Remote Desktop Protocol) and GoToAssist as these means utilize encrypted connections. FTP, email or non-secure means are not acceptable.

Data Storage & Disposal

In the event that data needs to be held in our secured data environment for a temporary period of time and our agreement with that client has expired, the data shall be deleted in its entirety within 90 days from the expiration of the agreement. Contracted client data must be stored in encrypted volumes in the event that remote diagnosis and/or troubleshooting steps prove unsuccessful and contracted client data has been securely transmitted to Finance Manager premises. Regular and random audits will be performed for contracted client data on employee workstations.

Email Use Policy

All employees must avoid the use of any email system to transmit sensitive, personally identifiable information. Sharefile should be utilized to transmit any data between clients and Finance Manager. Use of Finance Manager email systems for personal use is strictly prohibited.

Removable Media Policy

Removable media defined as USB thumb drives (flash drives), external hard drives, CDs, DVDs, and magnetic media should be handled with care to prevent loss or corruption. When not in use, media should be secured in a locked cabinet, drawer, etc. Flash drives should be formatted regularly and any other media should be destroyed when a support case has been closed. Flash drives should not be used to transport data outside Finance Manager premises as these drives can be misplaced or stolen.

Printing Policy

Any printed documents that are the result of testing or troubleshooting a support issue should be destroyed at close of the case, if not sooner.

Safeguarding Physical and Mobile Devices Policy

All employees must immediately notify an officer of Finance Manager in the event that a device containing in-scope data is lost (e.g., mobile phones, laptops, etc.). All assets holding data in scope should not be left unduly exposed, for example visible in the back seat of a car. As an added layer of protection in case of accidental loss or theft of devices such as laptops, tablets, workstations, etc., Finance Manager uses Absolute Computrace for remote tracking (geolocation), remote wipe, device freeze with message to user and theft recovery. Computrace is persistent and embedded into the device firmware. Even if the agent is unloaded, the persistence module will reinstall the agent automatically.

3.0 Policies - Continued_

Workstation/Laptop Safe Use Policy

During normal business hours, workstations, laptops, and tablets should be locked when not in use. Unless otherwise instructed, workstations should be powered down nightly. Outside of normal business hours, laptops and tablets should be secured in a locked cabinet, locked desk drawer or locked in the server room.

Name: Ronald J Bovich

Date: May 5, 2021

Signature: Ronald J. Bovich

Title: President