DATA SHARING AND CONFIDENTIALITY AGREEMENT (CONTINUED)

ERIE 1 BOCES

BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website: http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

BY THE VENDOR: MML D/B/A FINANCE MANAGER

Ronald J. Bovich

Signature

Ronald J. Bovich, President

Name/Title

6/29/20

Date

I, Ron Bovich, President of Finance Manager hereby state that my endorsement of the present document is pro forma. Finance Manager does not receive any PII student information. Nor can Finance Manager software be used in any way to personally identify any PII student information.

DATA SHARING AND CONFIDENTIALITY AGREEMENT (CONTINUED)

SUPPLEMENTAL INFORMATION ABOUT A CONTRACT BETWEEN MML DBA/FINANCE MANAGER AND ERIE 1 BOCES

Erie 1 BOCES has entered into a Contract with MML DBA/FINANCE MANAGER which governs the availability to Participating Educational Agencies of the following Product(s):

Finance Manager/nVision

Pursuant to this Contract, Participating Educational Agencies (*i.e.*, those educational agencies that are authorized to use the above Product(s) by purchasing certain shared technology services and software through a Cooperative Educational Services Agreement with Erie 1 BOCES) may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data"). Vendor has also entered into a separate Data Sharing and Confidentiality Agreement ("DSC Agreement") with Erie 1 BOCES setting forth Vendor's obligations to protect the confidentiality, privacy and security of Protected Data it receives pursuant to the Contract.

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to the Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized above or in the DSC Agreement. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the Contract (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the Contract and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [*see attached Vendor MML D/B/A Data Privacy and Security Plan*]

Duration of Contract and Protected Data Upon Expiration:

- The Contract commences on 2001 and renews annually.
- Upon expiration of the Contract without renewal, or upon termination of the Contract prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of any APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

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.

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: Any data that is held temporarily by Finance Manager is never to be disclosed to anyone outside of our company, unless disclosure is ordered by a court of law. Each employee at Finance Manager is required to sign a confidentiality agreement that outlines company policies for non-disclosure and handling of sensitive client data they may come in contact with during their employment.

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. 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: June 29, 2020

Signature: Ronald J. Bovich

Title: President