


## EXHIBIT B

### BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	Media Flex Inc.
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Library Management System
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <b>X Student PII</b> <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>08/15/2024</u>   Contract End Date <u>08/15/2025</u>
<b>Subcontractor Written Agreement Requirement</b>	<input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: • <b>Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties.</b> • <b>Securely delete and destroy data.</b>
<b>Challenges to Data Accuracy</b>	<b>Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.</b>
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)

<p>See Media Flex Data Privacy &amp; Security Plan article "5" - firewall &amp; intrusion protection HIPAA compliant - SFTP Protocol - Staff PII access limited to DP technicians -Staff PII access training</p>	<p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input checked="" type="checkbox"/> Contractor owned and hosted solution. <input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Information is only accessed by those necessary to perform Contractor obligations</p>
<p><b>Encryption</b></p>	<p><b>Data will be encrypted while in motion and at rest.</b></p>

<p><b>CONTRACTOR</b></p>	<p>Media Flex Inc.</p>	
<p>[Signature] </p>		
<p>[Printed Name] H. Chan</p>		
<p>[Title] President</p>		

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	PII data transmission to SFTP site.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	SFTP - HIPAA compliance - Proven Firewall - application login / pw
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Staff receive instruction to limit access to PII data only to persons with specific purpose for maintaining and processing such information.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	MF staff are required to acknowledge & adhere to PII data privacy policy. MF does not use subcontractors
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Please see Media Flex IT Security & Notification Plan: Pages 2-5 Scans: BurpSuite Pro - Nessus Pro - CISA Scan - MF will use NYS Ed Data Incident Reporting Form
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	MF Staff will remove all PII data & formally certify with EA IT staff
7	Describe your secure destruction practices and how certification will be provided to the EA.	MF data processing staff will remove all PII data & statistics & formally certify
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Security is provided on the data, application, and hosting level, firewall HIPAA compliant - Limited access to PII data to authorized tech support staff MF staff receive & acknowledge DOE PII policy instruction
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
<b>IDENTIFY (ID)</b>	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Employees who have access PI are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and received training on how to do so. HIPAA compliant firewall - Application includes transaction anonymization. Application vulnerability scans.
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	MF staff receive & acknowledge DOE PII policy instruction Programmers, data processing technicians, application tutors, and application clients are informed of PI priorities ex. <a href="https://docs.google.com/document/d/16SClaLLam2OJAAJ3jmhBnUwwz6iHnMSyfSNhsL7FJyl/edit">https://docs.google.com/document/d/16SClaLLam2OJAAJ3jmhBnUwwz6iHnMSyfSNhsL7FJyl/edit</a>
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	MF administrators and staff are informed by the NYSED policies, procedures and processes articulated by the Chief Privacy Officer: <a href="https://www.nysed.gov/data-privacy-security">https://www.nysed.gov/data-privacy-security</a>
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	MF administrators and staff are informed by the NYSED policies, procedures and processes articulated by the Chief Privacy Officer & CISA
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	MF administrators and staff use scans to detect vulnerabilities and intrusion attempts. Client data is backed up in multiple and off-site and is mirrored in regional union catalog databases.
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	MF - OPALS does not use third party developers or support staff. Power supply is backed up using natural gas generators.

Function	Category	Contractor Response
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Access, authentication and access control to physical and logical assets and facilities is limited to authorized users only.
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	MF staff receive PI and cybersecurity awareness training. Similar training and documentation is conveyed to clients using system applications and services.
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data security and records are managed using industry protocols and tools. SFTP, HIPAA protocols, admin authentication and hierarchical protocols provide access only to those who are authorized and "need to know."
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	MF data processing technicians work with EA IT staff to establish SFTP sites to receive encrypted data that authorized technicians map and upload to application student and teacher directories. MF technicians coordinate beginning and end of school year rollover and new student data uploads.
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	N/A
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Vulnerability scans are done weekly - backup generators are tested weekly and operational status or maintenance
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	IT verifies system for anomalies. Detected anomalies are reported to IT and application engineers for remediation.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	IT staff and utilities report cybersecurity attacks and deflected by monitoring equipment / technology.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	IT staff use Firewall hardware/scans to detect and report anomalies.



Function	Category	Contractor Response
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Please see MF IT Security Information and Notification Plan attached: Identification - Verification - Containment-Analysis, Recovery, Reporting, Data Retention
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Please see MFIT Security Information & Notification Plan Identification - Reporting
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Please see MF IT Security Information & Notification Plan Verification - Reporting
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Please see MF IT Security Information & Notification Plan Containment - Reporting
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Please see MF IT Security Information & Notification Plan Data Retention - Reporting
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Please see MF IT Security Information & Notification Plan Recovery - Reporting
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	Please see MF IT Security Information & Notification Plan Reporting - Data Retention
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Please see MF IT Security Information & Notification Plan Notification - Reporting - Data Retention

## **EXHIBIT A: DATA SHARING AND CONFIDENTIALITY AGREEMENT**

**Including**

**Forestville Central School District Bill of Rights for Data Security and Privacy and Supplemental Information about a Master Agreement between Forestville Central School District and Media Flex Inc.**

### **1. Purpose**

(a) **Forestville Central School District** (herein after “District”) and Media Flex Inc (hereinafter “Vendor”) are parties to a contract, Terms of Service, or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from the District for purposes of providing certain products or services to the District (the “Master Agreement”).

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District’s Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between **Forestville Central School District** and **Vendor** that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect

at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

## 2. **Definitions**

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

## 3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policies on data security and privacy.

## 4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.



Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between **Forestville Central School District** and **Vendor**. Vendor's obligations described within this section include, but are not limited to:

- i. its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and
- ii. its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

## 5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting **Wesley Wright, Director of Technology** directly by email at **wwright@forestville.com** or by calling **716-965-6565**.

(c) Vendor will cooperate with the District and provide as much information as possible directly to **Wesley Wright** or his/her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform **Wesley Wright** or his/her designee.

## 6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

- (i) the parent or eligible student has provided prior written consent; or
- (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To 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 permit another party to do so.

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

## **FORESTVILLE CENTRAL SCHOOL DISTRICT**

### **PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

The Forestville School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs 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 New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 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 Privacy Complaint, 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/student-data-privacy/form/report-improper-disclosure>.

### **APPENDIX**

#### Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Forestville School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security

requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 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;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- 6) Address how the data will be protected using encryption while in motion and at rest.

Adopted: 12/3/2020

---

BY THE VENDOR:

Media Flex Inc.

Name (Print)



Signature

President

Title

08 - 15 - 2024

Date