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 Media Flex, Inc. (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.

MEDIA FLEX, INC.

BY: A. Cohen **DATED:** 04/13/2021

DATA PRIVACY AND SECURITY PLAN

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

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

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.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, 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.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk 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 Eastern Suffolk 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 Eastern Suffolk 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.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

DATA PRIVACY AND SECURITY PLAN
Media Flex Inc.

Media Flex Inc. maintains a Data Security and Privacy Plan that includes the following elements congruent with New York State Education Law 2-d Rider for Data Privacy and Security:

1. New York State Libraries use OPALS Library Automation software to automate libraries in this region. Only data essential for providing library circulation, online public catalog, and member authentication services are uploaded.

2. Media Flex Inc. does not share, sell, rent or trade Personally Identifiable Information with third parties for promotional purposes on their part. Media Flex Inc. does not upload email addresses without the site visitor voluntarily providing the library with this information.

3. If a library were to terminate its contract with Media Flex Inc., Media Flex Inc. technical support staff would return any library data and destroy any data that might have been stored.

4. To prevent unauthorized access or disclosure, to maintain data accuracy, to allow only the appropriate exercise of a library's Personal Information while also protecting the confidentiality, integrity, and availability of user's Personal Information, Media Flex Inc. employs a variety of industry standard security technologies.

5. An outline of these security technologies is as follows:
   - Security is provided on the data, application, and hosting level to include a physically secure data center, proven firewall protection, and intrusion prevention measures which are HIPAA compliant.
   - Authorized library staff can specify levels of user security, using passwords and hierarchical assignment of such.
   - Media Flex Inc. limits access to user's Personal Information and data to those persons who have a specific purpose for maintaining and processing such information.

6. Media Flex Inc. employees who have access to user's Personal Information are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.

7. Media Flex Inc. does not hire or work with subcontractors

8. Media Flex Inc. technical support and computer engineering staff are cognizant of and trained to detect and diagnose as well as notify all parties with respect to security incidents. The Media Flex Inc. Data Breach and Notification Plan is appended.

Harry Chan
President

Media Flex Inc. - P.O. Box 1107 - Champlain, NY 12919

Media Flex IT Security Information and Notification Plan

Incident Handler: Media Flex Inc. technology security staff

System Administrator: Media Flex Inc. "First Responder"

System Owner: Context relevant (Could be Media Flex Inc. staff if hosted by MF… or client)

HIPPA Privacy & Security Officer: Media Flex Inc. security staff

Identification

Identify a potential incident: Incident handler monitors of security sensors. System owners or system administrators do so by observing suspicious system anomalies. Anyone in the library community may identify a potential security incident though external complaint notification.

Notify: Library community staff that suspect an IT system has been accessed without authorization must immediately report the situation to ctho@mediaflex.net As soon as the incident handler is aware of a potential incident, s/he will alert local system administrators.

Quarantine: The incident handler will quarantine compromised hosts when notified unless they are on a Quarantine Whitelist. If they are on a Quarantine Whitelist, the incident handler will contact the system administrator or system owner to contain the incident. Note that the incident handler alert parties of suspicious behavior when not confident of an incident; in these cases do not quarantine the host immediately, but wait 24-48 hours and quarantine only if the registered contact is unresponsive.

Verification

Classify: Critical Incident Response (CIR) procedures when...

1. The system owner or system administrator indicates that the system is a high-criticality asset
2. OR the system owner or system administrator alerts that the system contains Restricted Data
3. OR library staff determines that the system poses a unique risk warranting investigation.

Verify: The CIR process should be initiated when...

The incident handler verifies that the alert is not a false positive. The incident handler will double-check the triggering alert, and correlate it against other alerting systems when possible.

AND the type of data or system at risk is verified to be of an appropriate classification, as determined above. The system owner or system administrator should provide a detailed description of the data at risk, including approximate numbers of unique data elements at risk, and the number, location, and type of files it is stored in.

For the CIR process to be initiated the criticality of the asset must be confirmed, and it must be confirmed that the triggering event is not a false positive. In cases where the CIR process is not required, the incident handler can resolve the case as follows:

Obtain a written statement from the system owner or system administrator documenting that the system has no Restricted Data and is not a high-criticality asset.

Obtain a written statement from the system owner or system administrator that the system has been reinstalled or otherwise effectively remediated before quarantine is lifted.

For incidents involving an unauthorized wireless access point, obtain a written statement that the access point has been disabled.

Containment

1. If the host cannot immediately be removed from the network, the incident handler will **initiate a full-content network dump** to monitor the attacker's activities and to determine whether interesting data is leaking during the investigation.
2. **Eliminate attacker access:** Whenever possible, this is done via the incident handler performing network quarantine at the time of detection AND by the system administrator unplugging the network cable. In rare cases, the incident handler may request that network operations staff implement a port-block to eliminate attacker access. In cases where the impact of system downtime is very high, the incident handler will work with system administrators to determine the level of attacker privilege and eliminate their access safely.
3. The incident handler will collect data from system administrators in order to quickly **assess the scope of the incident**, including:
    1. Preliminary list of compromised systems
    2. Preliminary list of storage media that may contain evidence
    3. Preliminary attack timeline based on initially available evidence
4. **Preserve forensic evidence**:
    1. System administrators will capture **first responder data** if the system is turned on. The incident handler will provide instructions for capturing this data to the individual performing that task.
    2. The incident handler will capture disk images for all media that are suspected of containing evidence, including external hard drives and flash drives.
    3. The incident handler will dump network flow data and other sensor data for the system.
    4. The incident handler will create an **analysis plan to guide** the investigation.

The actions that need to be taken will depend on the uptime requirements of the compromised system, the suspected level of attacker privilege, the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the system(s) as quickly as possible and to preserve evidence for later analysis.

Additionally, this is the phase where the incident handler works most closely with system administrators and system owners. During this phase they are expected to take instruction from the incident handler and perform on-site activities such as attacker containment, and gathering first response data.

Analysis

The analysis phase is where in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of analysis is to establish whether there is reasonable belief that the attacker(s) successfully accessed Restricted Data on the compromised system. Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, and

relevant compliance officers. Questions which are relevant to making a determination about whether data was accessed without authorization include:

1. **Suspicious Network Traffic**: Is there any suspicious or unaccounted for network traffic that may indicate data exfiltration occurred?
2. **Attacker Access to Data**: Did attackers have privileges to access the data or was the data encrypted in a way that would have prevented reading?
3. **Evidence that Data was Accessed**: Are file access audit logs available or are file system mactimes intact that show whether the files have been accessed post-compromise?
4. **Length of Compromise**: How long was the host compromised and online?
5. **Method of Attack**: Was a human involved in executing the attack or was an automated "drive-by" attack suite employed? Did the tools found have capabilities useful in finding or exfiltrating data?
6. **Attacker Profile**: Is there any indication that the attackers were data-thieves or motivated by different goals?

Using these factors, the security officer will determine the degree of technical probability that the security or privacy has been compromised. Document each impermissible use and disclosure and the risk assessment conducted for each. That HIPPA Officer will be responsible for conducting the risk assessment, documenting the results of the assessment and whether the impermissible use or disclosure poses a significant risk of financial, reputational or other harm to the individual whose data was compromised.

Recovery

The primary goal of the recovery phase is to restore the compromised host to its normal function in a safe manner.

The system administrators will remediate the immediate compromise and restore the host to normal function.

The system administrators will make short-term system, application, and business process changes to prevent further compromise and reduce operating risk.

Reporting

The final report serves two main purposes. First, a recommendation is made as to whether the incident handler and the responsible officials feel there is a reasonable belief that Data was disclosed impermissibly without authorization and the degree of probability that security or privacy has been compromised. The report will be made to allow notification, if appropriate, within any legally-mandated time period. In the case of HIPAA/HITECH/Omnibus, that is within 60 days of discovering the Breach. Second, a series of mid-term and long-term recommendations will be made to the owners of the compromised system, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

1. The incident handler will draft the final report after the investigation is complete.
2. After the draft report is completed, signoff on the content of the report should be obtained from management. Technical personnel can offer comments as well.
3. For critical incidents involving payment card data, the PCI Compliance Manager will receive a copy of the report and appropriate entities will be notified in the event that cardholder data is accessed without authorization. The Compliance Manager will be responsible for all communication with the payment

card brands and will be responsible for coordinating the activities mandated by the payment card brands with respect to the incident.

4. For critical incidents, the report will include each impermissible use and disclosure and the risk assessment conducted for each.
5. The incident handler will schedule a meeting to deliver the final report to the system administrator and the system owner.
6. The incident handler will ensure that the final report includes the details of the investigation and mid-term and long-term recommendations to improve the security posture of the organization and limit the risk of a similar incident occurring in the future.

Data Retention

1. The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for six (6) years.
2. Incident notes should be retained for six (6) months from the date that the report is issued. This includes the investigation page, file-timelines and filtered network-flows.
3. Raw incident data should be retained for thirty (30) days from the date that the report is issued. This includes disk-images, unfiltered netflow-content, raw file-timelines, and other data that was collected but deemed not relevant to the investigation.

12/04/2020

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.

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.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, 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.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk 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;

To ensure proper access to the library service by authorized users only an identity verification system is utilized.

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;

   The contractor does not employ subcontractors.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   All library data will be returned and any stored data 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;

   They may contact their school administrator listed in the district's parent's bill of rights or they may contact the State's Chief Privacy Officer at New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

   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.

   All data is stored on the OPALS servers which reside at the Eastern Suffolk BOCES facility in Oakdale, New York. Media Flex Inc. limits access to user's Personal Information and data to those persons who have a specific purpose for maintaining and processing such information. Media Flex Inc. employees who have access to user's Personal Information are made aware of their responsibilities to protect the confidentiality, integrity, and availability of that information and have been provided training and instruction on how to do so.

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 Eastern Suffolk 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 Eastern Suffolk 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.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.