LOOM DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") supplements and is incorporated into the Loom Terms of Service or other agreement between School District of the Menominee Area (Customer") and Loom governing Customer's use of and access to the Services ("Agreement"). Capitalized terms used below that are not otherwise defined have the meanings given to them in the Agreement.

1. SCOPE

1.1 **Scope of DPA.** This DPA applies to Loom's processing of Personal Data to provide the Services to Customer pursuant to the Agreement.

1.2 **Processor.** The parties agree that Loom acts as a processor under Data Protection Law and/or service provider under CCPA for Customer in providing the Services to Customer.

1.3 **Processing Activities.** The subject matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, and categories of data subjects are described in Exhibit A.

2. PROCESSING OF PERSONAL DATA

2.1 **Loom Obligations.** Loom will:

(A) process Personal Data only on documented instructions from Customer, including transfers of Personal Data to a third country or an international organization, unless required to do so by applicable law to which Loom is subject, in which a case Loom will inform Customer of the legal requirement before processing, unless prohibited by law;

(B) ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(C) implement appropriate technical and organizational measures, including the Security Measures, which are attached hereto as Exhibit B, designed to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed and to ensure a level of security appropriate to the risk;

(D) respect the conditions for engaging other processors as required by applicable Data Protection Law and set forth in Section 4 below;

(E) taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, to the extent possible, to enable Customer to fulfill its legal obligations as a controller to respond to requests for exercising data subject rights pursuant to applicable Data Protection Law;

(F) taking into account the nature of processing and the information available to Loom, assist Customer in ensuring compliance with its legal obligations pursuant to applicable Data Protection Law regarding (i) security of processing, (ii) notification of and communication of Security Incidents, (iii) data protection impact assessments, and (iv) prior consultation with the applicable supervisory authority;

(G) at Customer's choice, delete or return all Personal Data to Customer after the end of the provision of the Services, and delete existing copies unless applicable law requires storage of Personal Data;

(H) make available to Customer all information necessary to demonstrate compliance with its obligations under applicable Data Protection Law and allow for and assist with audits in accordance with Section 6 below, in each case at Customer's expense; and

(I) inform Customer if, in its opinion, an instruction infringes applicable Data Protection Law.

2.2 **Customer Instructions**. Customer instructs Loom to process Personal Data as documented in this DPA and the Agreement, and as otherwise necessary to provide the Services to Customer. Customer's instructions to Loom for the processing of Personal Data will comply with all applicable laws, including Data Protection Laws.

2.3 **Controller Authorization.** If Customer is a processor, Customer warrants to Loom that Customer's instructions and actions with respect to Personal Data, including its appointment of Loom as a subprocessor, have been authorized by the relevant controller.

3. DATA TRANSFERS

3.1 **Customer Authorization.** Customer authorizes Loom to perform Data Transfers: (a) to any country subject to an adequacy determination by the European Commission; (b) pursuant to the Standard Contractual Clauses; or (c) any other legally valid data transfer mechanism. The Standard Contractual Clauses will only apply for Data Transfers to a country not recognized as having an adequate level of data protection if there is no other

legally valid data transfer mechanism.

3.2 **Standard Contractual Clauses**. For Data Transfers out of the European Economic Area, Switzerland, or the United Kingdom pursuant to the Standard Contractual Clauses: (a) where Customer acts as a controller of Personal Data, the Controller-to-Processor Clauses will apply; and (b) where Customer acts as a processor of Personal Data, the Processor-to-Processor Clauses will apply and Customer will fulfill any obligations Loom may have to Customer's controller(s) as a processor.

3.3 **UK Addendum.** For Data Transfers out of the United Kingdom, the UK Addendum will apply.

4. SUBPROCESSORS

4.1 **General Authorization.** Customer hereby grants Loom general authorization to engage Subprocessors, subject to the terms of this DPA and the Agreement. Loom uses the Subprocessors listed at www.loom.com/privacy to provide the Services and will notify Customer of any intended changes concerning the addition or replacement of a Subprocessor via the mechanism listed on that page. If Customer provides a reasonable written objection to a new Subprocessor within 10 days of receiving notice, and Loom chooses not to suggest an alternative, Customer may terminate the Agreement after 30 days' notice to Loom.

4.2 **Subprocessor Requirements.** Prior to the engagement of a Subprocessor, Loom will enter into a written agreement with the Subprocessor containing at least the same data protection obligations as those set out in this DPA, including providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of applicable Data Protection Law. If a Subprocessor fails to fulfill its data protection obligations, Loom will be liable to Customer for the performance of that Subprocessor's obligations.

5. SECURITY INCIDENTS

5.1 **Security Incident Notification.** Upon becoming aware of a Security Incident, Loom will notify Customer without undue delay and promptly take reasonable steps to minimize harm and secure Personal Data.

5.2 **Notification Description.** To the extent possible, notification to Customer will describe the nature of the Security Incident, the likely consequences of the Security Incident, and the measures taken or proposed to be taken to address the Security Incident. Loom's notification of or response to a Security Incident will not be construed as an acknowledgement by Loom of any fault or liability with respect to the incident.

6. AUDITS

6.1 **Customer Audit.** Upon Customer's prior written request and subject to the confidentiality obligations, Loom will allow Customer or an independent third-party auditor that is not a competitor of Loom to access information or inspect Loom's procedures relevant to the protection of Customer Data in order to audit Loom's compliance with this DPA.

6.2 **Process for Inspections.** Inspections may be conducted no more than once per year and only in a manner that does not interfere with Loom's normal business operations. Customer and Loom will mutually agree upon the scope, timing, and duration of the inspection, and Customer will reimburse Loom for reasonable fees associated with time spent on the inspection. Any deficiencies or reports created based on such access or inspection must be promptly shared with Loom and will be Loom's Confidential Information.

7. CCPA CERTIFICATION

Loom will not:

(A) sell Customer personal information;

(B) retain, use, or disclose any Customer personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing Customer personal information for a commercial purpose other than providing the Service; or

(C) retain, use, or disclose Customer personal information outside of the direct business relationship between Customer and Loom.

8. GENERAL

This DPA is subject to the terms of the Agreement, including without limitation, those regarding dispute resolution, limitation of liability, and termination. If any of the provisions of this DPA conflict with the provisions of the Agreement, the provisions of this DPA will prevail.

9. DEFINITIONS

9.1 "CCPA" means the California Consumer Privacy Act of 2018 and any legislation or regulation that amends,

replaces, or re-enacts it.

9.2 "Controller-to-Processor Clauses" means the standard contractual clauses between controllers and processors approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://cdn.loom.com/assets/marketing/controller-to-processor-clauses.pdf.

9.3 "Data Protection Law" means (a) the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data effective 25 May 2018 (the General Data Protection Regulation) and any legislation or regulation that amends, replaces, or re-enacts it; and (b) any other applicable data protection law or regulation of the European Union or the European Economic Area and their member states, Switzerland, and the United Kingdom.

9.4 "Data Transfer" means any transfer or onward transfer of Customer Personal Data out of the European Economic Area, Switzerland, or the United Kingdom to another country.

9.5 "Personal Data" means personal data contained in Customer Data that is subject to applicable Data Protection Law or the CCPA.

9.6 "Processor-to-Processor Clauses" means the standard contractual clauses between processors approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, available at https://cdn.loom.com/assets/marketing/processor-to-processor-clauses.pdf.

9.7 "Security Incident" means a breach of Loom's Security Measures causing the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by Loom;

9.8 "Standard Contractual Clauses" means the Controller-to-Processor Clauses or Processor-to-Processor Clauses, as applicable and as may be updated from time to time to the extent required by Data Protection Law.

9.9 "Subprocessor" means a third party engaged by Loom to processes Personal Data in order to provide parts of the Services under the Agreement.

9.10 "UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force on March 21, 2022, issued by the UK Information Commissioner's Office under Section 119A(1) of the Data Protection Act 2018, available at https://cdn.loom.com/assets/marketing/uk-addendum.pdf.

9.11 The terms "controller", "processor", "data subject", "personal data," "processing" and "appropriate technical and organizational measures" have the meanings provided in applicable Data Protection Laws.

9.12 The terms "business", "commercial purpose", "service provider", "sell" and "personal information" have the meanings provided in the CCPA.

This DPA is accepted and agreed to by the authorized representative of each party below:

LOOM, INC.

By: _____

Print Name: Sam Taylor

Title: VP, Sales & Success

Date: _____

CUSTOMER

DocuSigned by:
Katherine Krueger
84F0EB00C576410...

By: _____

Print Name: Katherine Krueger

Title: Director of Technology Services

Date: 7/19/2023

Exhibit A

Subject Matter of Processing	The subject matter of the processing is the Personal Data submitted to the Services by Customer pursuant to the Agreement.
Duration of Processing	The processing will continue until the expiration or termination of the Agreement, or as otherwise determined by Customer by deleting Personal Data from its account.
Nature and Purpose of Processing	Processing by Loom to provide the Services to Customer pursuant to the Agreement.
Types of Personal Data	Personal Data provided to Loom by Customer or its Authorized Users, including: ● Name, email address, and other account data; ● Video, audio, transcript data, and comments containing Personal Data; ● Transaction logs for transactions conducted by users using the Service; ● Information about the hardware and software used to access the Service; ● Information and analytics about use of the Service; ● Employee authentication information, such as user ID and department information; ● Other Personal Data uploaded or submitted by Customer or Authorized Users to the Services.
Categories of Data Subjects	Employees and other Authorized Users of Customer and any other individual whose Personal Data is uploaded or submitted by Customer or Authorized Users to the Services.

Exhibit B

Security Measures

Loom uses commercially reasonable efforts to implement and maintain the security measures listed below. Loom may update or modify these Security Measures from time to time provided that the updates and modifications will not result in any material degradation of the overall security of Loom's Services.

Personnel Security

- **Background Checks.** Loom conducts background checks for employees and contractors with systems access to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.
- **Confidentiality.** Loom personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Loom's internal policies.
- **Security Education and Awareness Training.** Loom personnel are required to attend security and privacy training upon hire and annually thereafter.

Organizational Security

- **Access Controls.** Loom implements access provisioning based on the principle of least privilege and access removal controls promptly upon termination.
- **Multi-factor Authentication (MFA).** Loom employs multi-factor authentication for access across our production environment and internal systems containing Customer Data.
- **Passwords.** Loom requires and enforces password complexity requirements where passwords are employed for authentication (e.g., login to workstations). These requirements include restrictions on password reuse and sufficient password strength.
- **Anti-Virus and Malware.** Loom employs an anti-virus and malware solution with daily signature updates for end user devices.
- **Endpoint Security.** Loom-issued devices are configured by Loom's endpoint management solutions which include inactivity screensaver timeouts, full disk encryption, remote data wipe and lock capabilities, and regular patching.
- **Information Security.** Loom personnel are required to acknowledge and comply with Loom Information Security policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of employment.
- **Monitoring and Incident Response.** Loom maintains incident detection capabilities and a documented incident response program. In the event of an incident, Loom will promptly take reasonable steps to minimize harm and secure Customer Data.

Data Practices

- **Industry Standard Encryption.** Data in transit is encrypted using TLS 1.2+, and data at rest is encrypted using AES-256. Loom hashes user passwords with bcrypt before storing them in an encrypted database.
- **Retention and Deletion.** Loom maintains backup data for up to 30 days after a video has been permanently deleted by an end user. Video data is then permanently deleted.
- **Secure Destruction.** Loom's primary hosting provider complies with Department of Defense standards for secure erasure and secure decommissioning of storage media.
- **Storage.** Loom stores data in a multi-tenant environment hosted on AWS servers and logically isolates Customer Data.

Network Protection

- **Firewalls.** Loom configures firewalls according to industry best practices and unnecessary ports and protocols are blocked by configuring AWS Security Groups and NACL (Network Access Control Lists). Configurations are regularly monitored using automated cloud security posture management tools.
- **Monitoring, Logging, and Alerting.** Loom logs application logs to monitor for any suspicious activity. This is done using an SIEM (Security Incident and Event Management) tool. All alerts are triaged by Loom's Security Team and a security incident is raised after log introspection.
- **AWS WAF (Web Application Firewall).** Loom uses AWS WAF for rate-limiting endpoints to prevent brute-force and DoS (Denial of Service) attacks. WAF is also used to configure ingress IP addresses for specific endpoints and to help Loom comply with U.S. export control laws and regulations.

Application Security

- **Vulnerability Scanning.** Loom has a robust vulnerability management program which is used to define security risk scores, severity ratings and SLAs. This program helps prioritize security fixes and identify compensating

controls.

- **Dependency Management.** Loom ensures both application level dependencies and OS level packages are updated regularly to patch security issues. Github Dependabot is used for application level libraries and AWS ECR (Elastic Container Registry) and Trivy (OSS) are used for OS level packages.
- **Static Application Security Testing (SAST).** Loom utilizes SAST to identify security vulnerabilities in our source code. This is integrated as a pull request level check in Github which preemptively identifies security issues before a branch is merged to Loom's main branch.
- **RBAC (Role Based Access Control).** Loom uses IAM (Identity and Access Management) policies to enforce strict access controls for employees to access customer personal data, videos and screenshots. All user activity is logged and monitored for anomalies.
- **Zero Trust.** Internal applications used by Loom personnel are secured using AWS Application Load Balancer's native integration with our identity provider. This is done using OpenID Connect which acts as an authentication layer over the OAuth 2.0 protocol. All access, permissions and scopes are defined centrally within our identity provider to manage and scale requests.

Data Hosting

- **Data Centers.** Loom hosts data on Amazon Web Services (AWS), which maintains internationally recognized world-class compliance certifications and reports. AWS maintains industry-leading security practices, offers state-of-the art environmental and physical protection for the services and infrastructure that comprise Loom's operating environment.
- **Backups.** Loom conducts periodic database backups. Backups are retained for 30 days during the normal course of operations.
- **Replication.** Loom also replicates databases and database backups in alternate availability zones. We perform regular backups and restoration testing.
- **Redundancy.** Loom's infrastructure has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. This design allows Loom to perform maintenance and improvements of the infrastructure with minimal impact on the production systems.
- **Business Continuity.** Loom replicates data across multiple systems to help protect against accidental destruction or loss.

Subprocessors

- **Due Diligence.** Loom conducts security reviews for vendors prior to onboarding to ensure adequate level of security, compliance, and privacy for the scope of services provided.
- **Confidentiality.** Loom takes appropriate steps to ensure our security posture is maintained by establishing agreements that require subprocessors and service organizations to adhere to confidentiality commitments.

Security Certifications and Reports

- **Security Compliance.** Loom works with an independent third party firm to ensure our security practices consistently meet industry best practices by performing regular SOC 2 audits in compliance with the 2017 Trust Services Criteria.
- **Penetration Testing.** Loom engages with independent third party firms to conduct application-level and network-level penetration tests at least annually. Results of these tests are shared with senior management, triaged, prioritized, and remediated in a timely manner.