# DATA PROCESSING AGREEMENT

**Between:** _____ ("LEA" or "School District")

**And:** Asan Digital LLC, dba UserAuthGuard ("Provider")

**Product:** UserAuthGuard — K-12 Chromebook Management Platform

**Effective Date:** _____

---

## ARTICLE I — PURPOSE AND SCOPE

**1.1 Purpose.** This Data Processing Agreement ("DPA") establishes the terms under which Provider collects, uses, maintains, and protects Student Data received from or on behalf of LEA through the UserAuthGuard platform. This DPA ensures compliance with the Family Educational Rights and Privacy Act ("FERPA"), the Children's Online Privacy Protection Act ("COPPA"), applicable state student data privacy laws, and industry best practices.

**1.2 Scope of Services.** Provider operates UserAuthGuard, a cloud-based K-12 Chromebook management platform that enables schools to assign devices to students, track check-in/check-out activity, manage device inventory, and recover lost or stolen devices. The complete description of services is set forth in Exhibit A.

**1.3 Applicability.** This DPA applies to all Student Data received by Provider from or on behalf of LEA, regardless of format. This DPA supplements the underlying service agreement between the parties. In the event of conflict, the terms of this DPA shall prevail over the service agreement with respect to Student Data.

## ARTICLE II — DEFINITIONS

**"Breach"** means the unauthorized acquisition, access, use, or disclosure of Student Data that compromises the security, confidentiality, or integrity of the data.

**"Commercial Purpose"** means to sell, use, or disclose data for advertising, marketing, building user profiles for non-educational purposes, or any purpose other than providing the contracted services to LEA.

**"COPPA"** means the Children's Online Privacy Protection Act, 15 U.S.C. 6501-6506, and its implementing regulations at 16 CFR Part 312.

**"De-Identified Data"** means data from which all personally identifiable information has been removed or obscured such that the remaining information does not reasonably identify an individual and re-identification is not possible.

**"Education Records"** has the meaning set forth in FERPA, 34 CFR 99.3.

**"FERPA"** means the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, and its implementing regulations at 34 CFR Part 99.

**"LEA"** means the Local Education Agency (school district or educational institution) entering this agreement.

**"Parent"** means a parent or legal guardian of a Student.

**"Personally Identifiable Information" or "PII"** has the meaning set forth in 34 CFR 99.3.

**"Provider"** means Asan Digital LLC, doing business as UserAuthGuard.

**"Student"** means any individual enrolled in or receiving services from LEA.

**"Student Data"** means PII from Education Records and any other information collected or maintained by Provider on behalf of LEA that directly relates to an identifiable current or former Student.

**"Sub-Processor"** means a third party engaged by Provider to process Student Data on behalf of Provider in connection with the services.

## ARTICLE III — STUDENT DATA OWNERSHIP AND CONTROL

**3.1 Ownership.** All Student Data remains the sole property of LEA. Provider acquires no ownership rights in Student Data.

**3.2 LEA Control.** LEA retains full decision-making authority over Student Data. Provider processes Student Data only in accordance with LEA's documented instructions and the terms of this DPA.

**3.3 Parental Access.** Provider shall respond to any LEA request for access to Student Data within 10 business days. Provider supports LEA's obligations under FERPA to provide parents with the right to inspect and review their children's education records. All parent requests are routed through LEA; Provider does not provide data directly to parents.

**3.4 Correction and Deletion.** Provider shall process LEA-directed corrections to Student Data within 30 business days. LEA may delete individual student records at any time through the UserAuthGuard admin dashboard or by written request to Provider.

## ARTICLE IV — AUTHORIZED ACCESS AND USE

**4.1 FERPA School Official Designation.** Provider is designated as a "school official" with a "legitimate educational interest" under FERPA (34 CFR 99.31(a)(1)). Provider:

- (a) Performs an institutional service or function for which LEA would otherwise use its own employees — specifically, managing and securing school-owned Chromebook devices;
- (b) Is under the direct control of LEA with respect to the use and maintenance of Education Records;
- (c) Uses Education Records only for the purposes for which disclosure was made; and
- (d) Complies with FERPA's re-disclosure requirements.

**4.2 Permitted Uses.** Provider may use Student Data solely to:

- (a) Provide the device management services described in Exhibit A;
- (b) Maintain and improve the security and functionality of the platform; and
- (c) Generate De-Identified or aggregated data for product improvement, provided re-identification is prohibited.

**4.3 Prohibited Uses.** Provider shall NOT:

- (a) Use Student Data for any Commercial Purpose;
- (b) Sell, rent, lease, or trade Student Data to any third party;
- (c) Use Student Data for targeted advertising or to build advertising profiles;
- (d) Use Student Data to create behavioral profiles of students unrelated to the contracted services;
- (e) Share Student Data with any third party except as authorized in this DPA;
- (f) Use Student Data in any manner inconsistent with this DPA or applicable law; or
- (g) Mine Student Data for any purpose not explicitly authorized by LEA.

**4.4 COPPA Compliance.** LEA provides consent on behalf of parents for Provider's collection of Student Data under COPPA's school consent provision (16 CFR 312.5(c)(3)). Provider relies on LEA to provide appropriate notices to parents regarding data collection. Provider collects only the minimum data necessary to perform the contracted services.

**4.5 Employee Access.** Access to Student Data is limited to Provider employees and contractors who have a legitimate need to know. All such individuals are bound by confidentiality obligations at least as protective as this DPA and have completed data privacy training.

## ARTICLE V — DATA COLLECTION LIMITATIONS

**5.1 Categories of Data.** The categories of Student Data collected by Provider are set forth in Exhibit B. Provider collects only the minimum data necessary to perform the services.

**5.2 No Excess Collection.** If Provider discovers it has collected data beyond what is specified in Exhibit B, Provider shall promptly notify LEA and delete the excess data.

**5.3 Purpose Limitation.** Student Data is collected exclusively for the purposes specified in this DPA and Exhibit A. Any new use of Student Data requires prior written consent from LEA.

## ARTICLE VI — DATA SECURITY

**6.1 Security Program.** Provider maintains a comprehensive information security program designed to protect the security, privacy, confidentiality, and integrity of Student Data.

### *6.2 Technical Safeguards.*

- (a) **Encryption in transit:** TLS 1.2 or higher for all data transmitted between users, the platform, and third-party services.
- (b) **Encryption at rest:** AES-256 encryption for all Student Data stored on Provider's systems.
- (c) **Access controls:** Role-based access control with unique user credentials. Multi-factor authentication required for all administrative access.
- (d) **Audit logging:** All access to Student Data is logged. Logs retained for a minimum of one year.
- (e) **Vulnerability management:** Regular vulnerability scanning, timely patching (critical patches within 48 hours).
- (f) **Network security:** Firewalls, intrusion detection, and DDoS protection measures.

### *6.3 Administrative Safeguards.*

- (a) Designated Privacy Officer responsible for data protection compliance.

- (b) Background checks conducted on employees with access to Student Data.
- (c) Annual data privacy and security training for all employees.
- (d) Written data handling policies and procedures.
- (e) Annual risk assessments.
- (f) Documented incident response plan, tested at least annually.

**6.4 Physical Safeguards.** Student Data is hosted on cloud infrastructure providers that maintain SOC 2 Type II certification, physical access controls, environmental controls, and redundant systems. All data is stored and processed within the United States.

### *6.5 UserAuthGuard-Specific Security Practices.*

- (a) **Device location data** is collected only on-demand when Lost Mode is activated by an authorized LEA administrator. Location is not continuously tracked.
- (b) **Device recovery screenshots** (Enterprise Chrome extension only) are captured only on-demand when a device is reported lost or stolen. Screenshots are stored encrypted and automatically deleted after 30 days or upon device recovery.
- (c) Provider does **not** engage in continuous screen monitoring, keystroke logging, browsing history collection, or application usage tracking.

## ARTICLE VII — DATA BREACH NOTIFICATION

**7.1 Notification Timeline.** Provider shall notify LEA within 72 hours of confirming a Breach involving Student Data. Notification shall be made by phone to LEA's designated contact, followed by written confirmation via email.

**7.2 Notification Contents.** Breach notification shall include:

- (a) Nature and circumstances of the Breach;
- (b) Categories and approximate number of students affected;
- (c) Description of the data elements compromised;
- (d) Likely consequences of the Breach;
- (e) Measures taken or proposed to contain and remediate the Breach; and
- (f) Contact information for Provider's designated point of contact.

**7.3 Provider Obligations.** Following a Breach, Provider shall take immediate steps to contain and remediate, cooperate with LEA's investigation, provide ongoing updates, maintain documentation for five years, and if attributable to Provider's negligence, bear the reasonable costs of notification and remediation.

**7.4 LEA Responsibilities.** LEA is responsible for notifying parents, students, and regulatory authorities as required by applicable law.

**7.5 State Law Compliance.** Provider shall comply with the Pennsylvania Breach of Personal Information Notification Act (73 P.S. 2301-2329) and any other applicable state breach notification laws.

## ARTICLE VIII — DATA RETENTION AND DELETION

**8.1 Retention During Agreement.** Provider retains Student Data only for the duration of the service agreement and as necessary to provide the contracted services.

**8.2 Deletion Upon Termination.** Within 30 calendar days of expiration or termination, Provider shall delete or destroy all Student Data including all copies, backups, and archived data. Provider shall provide written certification of deletion upon request.

**8.3 Data Export.** Prior to deletion, LEA may request an export of all Student Data in CSV or JSON format within 15 business days.

**8.4 Survival.** Provider's confidentiality and security obligations survive termination for three years. Breach notification obligations survive indefinitely.

## ARTICLE IX — SUB-PROCESSORS

**9.1 Approved Sub-Processors.** Provider's current Sub-Processors are listed in Exhibit C. Provider shall not engage any new Sub-Processor without 30 days prior written notice to LEA.

**9.2 Sub-Processor Obligations.** Provider enters into written agreements with each Sub-Processor imposing data protection obligations no less protective than this DPA. Provider remains fully liable for Sub-Processors.

**9.3 Objection Right.** LEA may object within 15 days. If unresolved, LEA may terminate upon 30 days notice.

## ARTICLE X — DUTIES OF LEA

**10.1 Compliance.** LEA shall comply with FERPA, COPPA, and applicable state laws, including providing required notifications to parents.

**10.2 Parental Consent.** LEA warrants it has provided notice and/or obtained consent as required under COPPA's school consent provision.

**10.3 Authorized Users.** LEA is responsible for ensuring only authorized personnel access the platform.

**10.4 Data Accuracy.** LEA is responsible for the accuracy and legality of Student Data provided to Provider.

## ARTICLE XI — GENERAL TERMS

**11.1 Governing Law.** This DPA shall be governed by the laws of the Commonwealth of Pennsylvania. Federal law (FERPA, COPPA) applies where applicable.

**11.2 Dispute Resolution.** Good-faith negotiation for 30 days, then mediation or litigation in Montgomery County, Pennsylvania.

**11.3 Term.** Co-terminus with the underlying service agreement.

**11.4 Termination for Breach.** Either party may terminate upon 60 days notice for material breach, with 30 days to cure.

**11.5 Order of Precedence.** (1) Applicable law; (2) this DPA; (3) Exhibits; (4) the service agreement.

**11.6–11.9** Amendment requires written signatures. Severability. No assignment without consent. Provider indemnifies LEA.

**11.10 Notices.** All notices shall be directed to:

**Provider:** Asan Digital LLC (dba UserAuthGuard), Attn: Privacy Officer, 13 Station Ave, Schwenksville, PA 19473. Email: privacy@userauthguard.com. Phone: (267) 639-8522

**LEA:** _____

---

## SIGNATURES

**ASAN DIGITAL LLC (DBA USERAUTHGUARD)**

Signature: _____

Name: Stef Verleysen

Title: Founder & Privacy Officer

Date: _____

**LOCAL EDUCATION AGENCY**

Signature: _____

Name: _____

Title: _____

Date: _____

# EXHIBIT A — DESCRIPTION OF SERVICES

**Service Name:** UserAuthGuard

**Service Description:** Cloud-based K-12 Chromebook management platform that enables schools to assign devices to individual students, track device check-in/check-out activity, manage device inventory, enforce organizational unit policies through Google Workspace integration, and recover lost or stolen devices.

### *Core Features (All Plans):*

1. 1:1 student-to-device assignment with automatic OU policy enforcement
2. Device check-in and check-out logging
3. Device inventory tracking and status management
4. Visual Google Workspace OU explorer and management
5. Bulk device assignment and transfer tools
6. Group policy management
7. Active device hours configuration
8. Support queue and repair queue management
9. Compliance reporting and audit logs
10. Administrator dashboard with real-time device status

### *Lost Mode (All Plans):*

- On-demand device location lookup
- Remote device lock
- Device recovery workflow management

### *Enterprise Extension Features (Optional):*

- Device recovery screenshot — on-demand screen capture for stolen device recovery only
- Content blocking — configurable site and category blocking
- Active device hours enforcement via extension

# EXHIBIT B — SCHEDULE OF STUDENT DATA

### *Data Collected:*

| Category | Data Elements | Source | Purpose |
|---|---|---|---|
| Student Identity | First name, last name, school email, student ID, grade, school | Google Workspace (via LEA) | Device assignment |
| Device Assignment | Serial number, asset tag, model, student mapping, dates | LEA admin + Google Admin | 1:1 device management |
| Check-In/Out | Timestamps, student ID, staff ID, condition notes | LEA staff actions | Device accountability |
| Device Location | GPS/Wi-Fi coordinates | Device (on-demand only) | Lost device recovery |
| Recovery Screenshot | Screen capture (Enterprise only) | Device (on-demand only) | Theft investigation |

**Data NOT Collected:** Grades, test scores, health records, disciplinary records, SSNs, financial data, biometrics, browsing history, keystroke logs, continuous screenshots, app usage, communications, social media, search history, file contents.

## EXHIBIT C — LIST OF SUB-PROCESSORS

| Sub-Processor | Purpose | Data Processed | Location |
|---|---|---|---|
| Amazon Web Services | Cloud infrastructure, hosting | All Student Data | United States |
| Amazon SES | Transactional email | Admin email addresses | United States |
| Google Workspace | Directory integration | Names, emails, OUs | United States |
| Stripe, Inc. | Payment processing | Billing info only — No Student Data | United States |

## EXHIBIT E — USERAUTHGUARD PRIVACY COMMITMENTS

**1. No Advertising.** UserAuthGuard does not display advertisements to students and does not use Student Data for advertising purposes of any kind.

**2. No Data Sales.** Asan Digital LLC does not and will never sell, rent, lease, or trade Student Data to any third party for any reason.

**3. No Commercial Use.** Student Data is used exclusively to provide the contracted device management services. Period.

**4. No Student Profiling.** UserAuthGuard does not build behavioral, psychological, or commercial profiles of students.

**5. No Continuous Monitoring.** UserAuthGuard does not continuously monitor student screens, capture scheduled screenshots, log keystrokes, track browsing history, or monitor application usage.

**6. No Continuous Location Tracking.** Device location is collected only on-demand when Lost Mode is activated.

**7. Minimal Data Collection.** Only the data elements listed in Exhibit B are collected.

**8. US Data Residency.** All Student Data is stored and processed within the United States.

**9. Transparency.** Provider maintains a publicly accessible privacy policy at userauthguard.com/privacy-policy/

**10. Accountability.** Provider will participate in an annual data privacy review with LEA upon request at no additional charge.

---