Data & Consent Policy

Effective Date: November 14, 2025
Company: SmileSafe AI LLC ("**SmileSafe AI**," "**we**," "**us**," "**our**")
Address: 1401 Hesters Crossing Road, Round Rock, TX 78681, USA
Contact: info@smilesafeai.com

This Data & Consent Policy explains what information we collect, how we obtain and document consent, and how organizations, parents/guardians, residents, and staff can manage choices when using SmileSafe AI websites, apps, scanners/kiosks/pods, and dashboards (the "**Services**"). This Policy works together with our **Privacy Policy**, **Cookie Policy**, and applicable agreements (e.g., MSA, DPA/BAA).

---

1) Scope & Roles

- **Organizations (schools, districts, senior residences).** For student/resident data, the organization is the primary data controller/covered entity; SmileSafe AI acts as a **service provider/processor** under our agreement.
- **Website visitors & prospects.** For marketing pages and demo requests, SmileSafe AI acts as a controller/business.
- **Care networks.** When enabled by an organization, we may exchange limited data with dental providers to facilitate referrals.

---

2) Categories of Data

Depending on configuration and local law, the Services may process:

1. **Account & admin data:** staff names, roles, emails, SSO IDs, permissions.
2. **Screening data:** images captured by hardware, AI-generated indicators/scores, symptom inputs, notes, timestamps.

3. **Care coordination data:** referral status, provider details, follow-up outcomes (if recorded).
4. **Family communication & consent data:** parent/guardian/resident name, contact info, language preference, consent/grant/withdrawal records, delivery receipts of summaries.
5. **Operational data:** device logs, usage analytics, security/audit logs, support tickets.
6. **De-identified/aggregated data:** metrics used to evaluate accuracy and improve the Services.

We do **not** require precise geolocation, SSNs, or payment card numbers for screenings.

---

3) Legal Bases & Consent Types

We rely on one or more of the following, depending on jurisdiction and your organization's settings:

- **Consent** (e.g., parent/guardian signature for students; resident or legal representative consent in senior care).
- **Performance of a contract** (providing the Services to your organization).
- **Legitimate interests** (security, fraud prevention, service improvement) balanced with data subject rights.
- **Legal obligation** (complying with law, audits, or safety notifications).

Where laws require **opt-in consent** for specific processing (e.g., certain screenings, communications, or use of non-essential cookies), we will collect, record, and honor that consent as configured by the organization.

---

4) Collecting & Recording Consent

Organizations select the consent model. We provide tools to help:

- **Digital consent forms** (mobile/desktop), signature capture, date/time stamp, signer identity, and language selection.
- **Paper-to-digital upload** (scan/photo) with metadata.
- **Role-based access** so only authorized staff can view or update consent status.
- **Audit trails** for grant, denial, or withdrawal of consent.
- **Versioning** to track which policy/form was accepted.
- **Multi-language summaries** to support comprehension.

No screening occurs where consent is required and not obtained or is withdrawn, per org configuration.

---

5) Minors, Students & Residents with Representatives

- **K-12 settings:** The school/district is responsible for obtaining parental consent where required (e.g., FERPA, state student privacy laws). We support consent collection and verification but do not replace the institution's obligations.
- **Senior residences:** Residents provide consent unless a legally authorized representative must consent.
- **Capacity concerns:** If a resident/student lacks capacity, organizations determine appropriate procedures consistent with law.

---

6) Managing Choices (Opt-Out/Withdrawal)

Individuals or their authorized representatives may:

- **Withdraw consent** for screenings or communications at any time via the links provided, consent portal, or through the organization; withdrawal does not affect prior lawful processing.
- **Choose communication channels** (email/SMS/paper) and language preferences.

- **Request access/correction/deletion** of organization-managed data by contacting the organization; we support them in fulfilling requests.
- **Marketing emails** from SmileSafe AI (website leads) include an unsubscribe link.

---

7) Data Use Purposes (Summary)

- Provide screenings, guidance, and reports configured by the organization.
- Facilitate referrals to dental providers, when enabled.
- Deliver summaries to families/caregivers in selected languages.
- Operate, secure, and improve the Services and models (including de-identified analytics).
- Comply with law, enforce agreements, and protect safety.

We do **not** sell personal information.

---

8) Sharing & Disclosures

We disclose data only as described:

- **Service providers/processors** under confidentiality and data-use limits (hosting, storage, analytics, security, translations, SSO).
- **Dental providers/care networks** when your organization enables referrals and shares necessary information.
- **The administering organization** (staff with appropriate permissions).
- **Legal/safety** and **corporate transactions** with appropriate safeguards.
- **De-identified/aggregated** insights for program evaluation.

---

9) Data Retention & Deletion

- Retention follows the organization's settings and our agreement; we keep consent records for legal/audit requirements.
- Upon authorized request from the organization, we provide **export** and support **deletion** or **anonymization** consistent with law and contractual obligations.
- Backups are purged on a rolling schedule.

---

10) Security & Access Controls

We use administrative, technical, and physical safeguards, including encryption in transit, access controls with MFA support, least-privilege roles, network isolation, logging, and vulnerability management. Organizations should enforce strong staff practices (unique logins, timely off-boarding).

---

11) Incident Response & Notifications

We maintain an incident response plan. If we become aware of a security incident affecting organization data, we will notify the impacted organization without undue delay and cooperate on required notifications per law and contract.

---

12) Cross-Border Transfers

Data may be processed in the United States and other locations. Where required, we use appropriate safeguards (e.g., Standard Contractual Clauses) and ensure processors meet comparable protections.

---

13) Research & Model Improvement

We may use **de-identified or aggregated** data to evaluate program impact and improve algorithms. We do not publish information that identifies an individual. Any identifiable research use would require additional approvals/consents as applicable.

---

14) Audits, Assessments & Agreements

Upon reasonable request from an organization, we provide security/privacy documentation, complete questionnaires, and enter into required agreements (e.g., **DPA**, **BAA**) where legally applicable to the deployment.

---

15) Updates to this Policy

We may revise this Policy from time to time. Material changes will be communicated via the dashboard or email to administrators. Continued use after the effective date constitutes acceptance.

---

16) Contact

Questions about data or consent?

SmileSafe AI LLC
1401 Hesters Crossing Road, Round Rock, TX 78681, USA
Email: info@smilesafeai.com