

WEBSITE PRIVACY POLICY

Website-only scope. This Policy applies to the public pages of makeasmile.com. It does not govern information submitted after signing in to any linked third-party patient portal. Do not use a public Website form for an emergency or to send highly sensitive medical, dental, financial, or account information.

1. Scope and Purpose

This Website Privacy Policy ("Policy") explains how Make a Smile Dental ("Make a Smile," "we," "us," or "our") collects, uses, discloses, and retains Personal Information through the public pages and public forms of makeasmile.com (the "Website"). It applies to Website visitors, prospective and current patients, parents and guardians, job applicants, vendors, and other persons who interact with the public Website. The Website is operated from the United States and is intended for United States residents, and Personal Information collected through the Website may be processed and stored in the United States.

For purposes of this Policy, "Personal Information" means information that identifies, relates to, describes, or can reasonably be linked with a particular person or household. It does not include information that is lawfully deidentified, aggregated, or publicly available under applicable law.

Information maintained by a dental practice as part of a patient record may be governed by the Health Insurance Portability and Accountability Act (HIPAA), the California Confidentiality of Medical Information Act, other healthcare privacy laws, and the applicable Notice of Privacy Practices. This Policy is not a medical-information authorization, consent to treatment, or substitute for any notice or authorization required by healthcare law.

2. Information We Collect

2.1 Information You Provide

Depending on how you use the Website, we may collect the following categories of Personal Information:

- Contact and inquiry information, such as your name, email address, telephone number, mailing address, preferred practice location, preferred method of contact, and the content of a message or request.
- Service-interest and referral information included in an inquiry or communication, such as the type of service of interest, preferred location, timing preferences, referral details, and information needed to route or respond to the request. A Website submission does not by itself confirm an appointment.
- Career and applicant information, such as your name, contact information, resume, work history, education, professional licenses or credentials, references, availability, work authorization, preferred locations, travel preferences, application responses, uploaded documents, and communications concerning employment opportunities.
- Feedback and correspondence, including comments, reviews submitted directly to us, complaints, support requests, and other communications concerning the Website or our services.
- Information you voluntarily include in a message or upload. You should not submit sensitive medical, dental, financial, government-identifier, password, or payment-card information

through a general public form unless the form specifically requests it and is intended for that purpose.

- Privacy and communication choices, including cookie preferences, opt-in or opt-out selections, and records of when and how a choice was made.

2.2 Information Collected Automatically

When you visit the Website, we and providers that support the Website may automatically collect:

- Device and network information, such as Internet Protocol address, browser type, operating system, device type, language, mobile carrier, and device or cookie identifiers.
- Website activity information, such as pages viewed, links selected, referring and exit pages, dates and times, time spent, navigation paths, form interactions, and error or performance information.
- Approximate location information inferred from an Internet Protocol address.
- Cookie, analytics, security, and diagnostic information used to remember settings, measure Website use, protect forms, detect abuse, troubleshoot problems, and maintain Website availability and security.

2.3 Information from Other Sources

We may receive Personal Information from persons acting for you, referral sources, publicly available sources, and providers that support Website hosting, forms, communications, recruiting, analytics, security, or related functions. We use information received from other sources only for purposes consistent with this Policy, the context in which it was collected, and applicable law.

3. How We Use Personal Information

We may use Personal Information to:

- Operate, maintain, secure, troubleshoot, and improve the Website and its public forms.
- Respond to questions, feedback, complaints, appointment inquiries, service requests, and other communications; route a request to the appropriate practice location or authorized personnel; and follow up about the request.
- Evaluate job applicants, communicate about employment opportunities, verify application information where lawful, and administer recruiting activities.
- Remember preferences, measure Website performance, understand how visitors use the Website, improve navigation and content, and evaluate Website features and outreach.
- Detect, investigate, prevent, and respond to fraud, misuse, malicious activity, security incidents, technical failures, and threats to persons, systems, or property.
- Comply with applicable law, legal process, professional obligations, regulatory requests, audits, record-retention requirements, and lawful requests from government authorities.
- Establish, exercise, or defend legal rights and claims; enforce applicable terms; obtain professional advice; and manage insurance, compliance, or risk matters.
- Support a proposed or completed merger, acquisition, financing, reorganization, sale, transfer, or similar business transaction, subject to applicable law and confidentiality protections.

- Create and use deidentified or aggregated information for lawful operational, analytical, security, quality-improvement, and planning purposes.

4. Cookies and Similar Technologies

The Website uses cookies and similar technologies to provide core functions, remember privacy choices, protect forms, measure performance, understand Website use, and support enabled Website features. These technologies may be placed by us or by providers that support the Website.

Strictly necessary technologies support functions such as page loading, traffic routing, security, fraud prevention, and storage of cookie preferences. Analytics and other third-party technologies may collect device identifiers and Website activity information to measure performance and understand how the Website is used.

The Website provides a cookie-settings tool that allows visitors to accept, reject, or manage nonessential cookies when those choices are available. Cookie choices are generally specific to the browser and device used. Clearing cookies, using another browser or device, or resetting browser settings may require you to make your choices again. You may also use browser controls to block or delete cookies, although parts of the Website may not function correctly if necessary technologies are blocked.

4.1 Do Not Track and Cross-Site Activity

Because there is no uniform industry standard for browser "Do Not Track" signals, the Website does not currently respond to those signals as a separate privacy request. Other parties may collect information about a visitor's online activities over time and across different websites when their analytics, embedded, advertising, or similar technologies are enabled on the Website. You may use the Website's cookie-settings tool and available browser controls to manage those technologies. To the extent applicable law requires recognition of a valid opt-out preference signal, we will process the signal as required by law.

5. How We Disclose Personal Information

We may disclose Personal Information in the following circumstances:

- **Authorized personnel and practice locations.** We may disclose information to our personnel, providers, practice locations, and authorized agents who need it to respond to a request, administer the Website, evaluate an application, support operations, or provide or coordinate requested services.
- **Service providers and contractors.** We may disclose information to providers that perform services for us, including Website hosting, cloud services, information technology, cybersecurity, forms, communications, recruiting, analytics, accessibility support, document management, and professional services. These providers may use information only as permitted by their role, contract, and applicable law.
- **Professional advisers and insurers.** We may disclose information to attorneys, accountants, auditors, consultants, insurers, and other advisers when reasonably necessary for legal, compliance, financial, risk, or claims purposes.
- **Legal, regulatory, and safety purposes.** We may disclose information when required or permitted by law, legal process, court order, subpoena, regulatory request, or professional obligation, or when reasonably necessary to protect rights, safety, systems, property, or the integrity of our services.

- **Business transactions.** Information may be disclosed to actual or prospective parties and advisers in connection with a merger, acquisition, financing, reorganization, bankruptcy, sale, transfer, or similar transaction, subject to applicable law and appropriate confidentiality protections.
- **At your direction or with permission.** We may disclose information to a person or service you ask us to contact, or when you provide consent or authorization that is valid for the disclosure.
- **Deidentified or aggregated information.** We may disclose information that has been lawfully deidentified or aggregated so that it is not reasonably capable of identifying a person.

6. Third-Party Patient Portal and Websites

The Website may link to a third-party patient portal used for scheduling, forms, messaging, records, payments, and other patient functions. Any such portal is operated by an independent company, not by us, and this Policy does not govern it. Information submitted through a patient portal is governed by that portal's own privacy policy, terms, and related agreements. The Website may also contain links to, or display content from, third-party websites and services that we do not control. We are not responsible for the privacy practices or content of third-party websites or services, and you should review the privacy policy of any third-party website or service before providing information to it.

7. Sale, Sharing, and Advertising-Related Disclosures

We do not use the Website to sell Personal Information in exchange for money. The Website may use analytics, cookie, advertising, embedded-content, or similar technologies that allow providers of those technologies to collect or receive identifiers, device information, and Website activity information for functionality, security, analytics, measurement, or advertising-related purposes.

Some privacy laws define "sale," "sharing," or targeted advertising broadly enough to include certain technology-enabled disclosures even when no money changes hands. To the extent such a law applies, we will provide and honor the opt-out, limitation, or preference-signal choices required by that law. We do not knowingly sell or share the Personal Information of a person under 16 without the authorization required by applicable law.

8. Children's Information

The public Website is intended for adults seeking information for themselves or for a child in their care. It is not directed to children under 13, and a child under 13 should not independently submit Personal Information through the public Website. A parent, legal guardian, or other legally authorized adult may provide information concerning a child when requesting information or services.

If we learn that Personal Information was collected online directly from a child under 13 in a manner requiring parental consent, we will take reasonable steps to comply with applicable notice, consent, access, retention, and deletion requirements. A request involving information that has become part of a patient record, billing record, legal hold, security record, or other record subject to a separate legal retention duty will be handled under the law governing that record.

9. Data Security

We use administrative, technical, and physical safeguards designed to protect Personal Information in light of the nature of the information, the systems involved, and applicable legal requirements. These safeguards may include access restrictions, authentication, monitoring, secure configuration, vendor controls, and incident-response procedures appropriate to the Website and the information processed.

No method of Internet transmission, electronic storage, or security is completely reliable. We therefore cannot guarantee that the Website or any information will be immune from unauthorized access, loss, misuse, alteration, interception, malware, or other security events. This statement does not limit any security or notification duty imposed by law.

Use a trusted device and network, verify that you are on the correct Website before submitting information, and report suspected phishing, impersonation, or Website security concerns using the contact information in Section 14.

10. Retention and Deletion

We retain Personal Information for as long as reasonably necessary and proportionate to the purpose for which it was collected or another compatible and lawful purpose. Relevant considerations may include the need to respond to requests, maintain business and communication records, evaluate applicants, protect security, prevent fraud, resolve disputes, satisfy legal, professional, tax, employment, audit, insurance, or recordkeeping obligations, enforce rights, and preserve evidence or comply with a legal hold.

Retention periods may differ depending on the category and context of the information. When information is no longer reasonably needed and deletion is permitted, we may delete, destroy, deidentify, or aggregate it. Copies may remain temporarily in backups, logs, archives, or systems subject to restricted use until they are deleted or overwritten through ordinary processes.

11. Your Choices and Privacy Requests

- **Cookie choices.** Use the Website's cookie-settings tool and available browser controls to manage cookies and similar technologies.
- **Communication choices.** You may use an unsubscribe or opt-out method included in an eligible marketing communication. Operational, security, legal, appointment-related, or other requested communications may continue as permitted by law.
- **Review or correction.** You may ask us to review or correct Personal Information collected through a public Website form by contacting us. We may verify your identity and authority before acting on a request.
- **Deletion or restriction.** You may request deletion or restriction where applicable law provides that right. We may retain information when permitted or required for legal compliance, patient or employment records, security, fraud prevention, audits, disputes, legal holds, or other lawful purposes.
- **Representatives.** A parent, guardian, personal representative, or other person acting for someone else may be required to provide proof of identity and legal authority. Additional requirements for authorized agents submitting California privacy requests are described in Section 11.1.

- **Patient records.** Requests concerning medical or dental records, billing records, or other patient records must be made through the applicable practice records process. A Website privacy request does not replace a legally required patient-record procedure.

We may deny, limit, or defer a request to the extent permitted by law, including when the request cannot be verified, concerns another person, would compromise security, seeks privileged information, conflicts with a legal hold, or concerns information that must be retained. We will not unlawfully discriminate or retaliate against a person for exercising an applicable privacy right.

11.1 Authorized Agents

If you submit a privacy request on behalf of another person, we may require signed, written permission from that person authorizing you to act on the specific request, together with proof of your identity, and, where permitted by law, we may require the person who is the subject of the request to verify their identity directly with us or to confirm directly with us that they authorized the request. These confirmation requirements generally do not apply when the agent acts under a valid power of attorney recognized by California law, and we will not require a power of attorney solely because a person chooses to use an authorized agent. An authorized agent must protect information obtained in connection with a request and use it only to submit or fulfill the request, complete verification, or prevent fraud. We may deny or limit a request when we cannot reasonably verify the agent's identity or authority or when otherwise permitted by law.

12. California Privacy Disclosures

12.1 California Online Privacy Policy Requirements

For California's online privacy-policy requirements, the categories of Personal Information collected through the Website are described in Section 2, and the categories of persons or entities with whom that information may be disclosed are described in Section 5. The process for requesting review or correction is described in Section 11. The process for material policy changes is described in Section 13. The Last Updated date shown at the top of each page is the date this Policy took effect. The Website's response to Do Not Track signals and disclosure concerning collection over time and across websites appear in Section 4.1.

12.2 Additional California Rights When Applicable

To the extent the California Consumer Privacy Act, as amended, applies to us and to the Personal Information at issue, a California resident may have rights to request information about collection, use, disclosure, sale, or sharing; access specific Personal Information; request correction or deletion; opt out of sale or sharing; limit certain uses or disclosures of Sensitive Personal Information; and receive equal service without unlawful discrimination for exercising a privacy right. These rights are subject to verification, statutory exceptions, and the scope of the law.

To the extent those requirements apply, during the 12 months preceding the Last Updated date, we collected through the Website the categories of Personal Information described in Section 2, from the sources described in Section 2, for the purposes described in Section 3, and disclosed that information to the categories of recipients described in Section 5. Sale- and sharing-related practices are described in Section 7.

A California privacy request may be submitted by email, telephone, or mail using the contact information in Section 14 or through any additional request method made available on the Website. We may request information reasonably necessary to verify identity, California residency, authority,

and the scope of the request. Requests are subject to applicable exceptions, verification requirements, and legal limitations.

12.3 California Sensitive Personal Information Disclosure

Under California law, Sensitive Personal Information may include government identifiers; account credentials; precise geolocation; racial or ethnic origin; citizenship or immigration status; religious or philosophical beliefs; union membership; the contents of certain communications; genetic, neural, biometric, health, sex-life, or sexual-orientation information; and Personal Information of consumers known to be under 16. Depending on the Website feature used and the information voluntarily provided, we may collect limited Sensitive Personal Information, such as health or dental information included in a message, the contents of communications directed to us, work-authorization or similar applicant information, or information concerning a child provided by an authorized adult.

We use and disclose Sensitive Personal Information collected through the public Website only as reasonably necessary and proportionate to provide requested Website functions or services, respond to communications, evaluate applications, protect security and integrity, prevent fraud or unlawful activity, ensure safety, comply with law, and carry out other purposes permitted by applicable law. We do not collect or process Sensitive Personal Information through the public Website for the purpose of inferring characteristics about a consumer. If our practices change so that California law requires a separate right to limit a use or disclosure of Sensitive Personal Information, we will provide the legally required notice and request method.

12.4 California "Shine the Light" Requests

California Civil Code section 1798.83 may permit a California customer who has an established business relationship with us to request information about specified categories of Personal Information, if any, that we disclosed to third parties for the third parties' direct-marketing purposes during the immediately preceding calendar year, together with the names and addresses of those third parties.

To submit a request, send a written request labeled "California Shine the Light Request" by email to info@makeasmile.com. Include your name, current California address, and enough information for us to identify your relationship with us and the information requested. We may require reasonable verification. We will respond to one qualifying request per customer per calendar year as required by applicable law. We do not disclose Personal Information to third parties for their own direct-marketing purposes unless the customer has affirmatively agreed or the disclosure is otherwise permitted by law.

13. Changes to This Policy

We may revise this Policy prospectively to reflect changes in law, Website features, technology, vendors, or privacy practices. The revised Policy will be posted on the Website and will identify a new Last Updated date, which is the date the revised Policy takes effect. When a change is material, we may provide additional notice through the Website or another method appropriate to the change and required by law. We will obtain consent before applying a material change to previously collected information when applicable law requires consent.

14. Contact Information

Questions, requests, or complaints concerning this Policy may be directed to:

Privacy Contact: Make a Smile Dental

Address: 2190 East Bidwell Street, Folsom, CA 95630

Email: info@makeasmile.com

Telephone: (916) 984-0304

Website: makeasmile.com

Do not include urgent medical information, payment-card information, passwords, government identifiers, or other highly sensitive information in an ordinary email. For a medical or dental emergency, call 911 or obtain local emergency care.