

Privacy Policy

NEURICA LTD trading as TheDentalBot

1. Who we are and when this policy applies

TheDentalBot is a trading name of NEURICA LTD, a company registered in England and Wales under company number 16747562. Our registered office is 20 Maybridge Crescent, Goring By Sea, Worthing, England, BN12 6HQ. In this policy, 'we', 'us' and 'our' mean NEURICA LTD.

This policy explains how we handle personal information through thedentalbot.co.uk, the equivalent TheDentalBot website at thedentalbot.com, our public chatbot demonstration, business enquiries, client administration and support. Our privacy contact is **enquiries@thedentalbot.co.uk**. You can also write to our registered office, marked 'Privacy enquiry'.

We are the controller for our own website, demonstration and business activities: we decide why and how that information is used. The demonstration uses an example practice and does not provide dental care.

A dental practice using TheDentalBot for its patients is normally their data controller. We process patient information on its documented instructions under a Data Processing Agreement. See section 5 and the practice's privacy notice for its patient record arrangements.

Read this with our Cookies Policy and Website Terms of Use. Reading a policy or accepting website terms is not consent to optional cookies, direct marketing or the processing of health information.

2. Information we collect and where it comes from

Website enquiries. The enquiry form asks for your full name, practice name, email address, practice postcode and message. A telephone number is optional. We receive the details you enter, subsequent correspondence and information needed to investigate a failed or abusive submission. The form sends submissions to a Supabase function for processing. Please keep messages relevant to your business enquiry and do not include patient records or clinical histories.

Business relationships. When you arrange a demonstration, discuss a service, become a client or ask for support, we receive business contact details, job roles, practice details, correspondence and service preferences. Contract records can include the signatory's name, role, signature, signing date and signing audit information. Billing records include the relevant business, invoice and payment administration details. We may receive your details from a colleague acting for your practice or from correspondence involving you.

Public demonstration. We receive the messages and selections you enter, the chatbot's responses, session identifiers, timestamps and interaction information. If you test an enquiry or confirmation email workflow, this can also create a structured enquiry record and an email containing the details you supplied. See section 4 before entering information.

Website and security information. Website and service providers process technical request information such as IP address, browser and device details, requested pages, timestamps and error or security events to deliver and protect the site. Loading externally hosted fonts also sends the information needed to request those fonts to Google.

Analytics and cookie choices. With Statistics consent, Google Analytics collects browser identifiers and information about pages viewed, interactions, device characteristics and how a visit reached the site. Cookiebot records your consent choice and related evidence, including the site, choice time, browser information and a consent identifier. Information about these technologies is in our Cookies Policy.

You can browse the ordinary public website without submitting an enquiry or accepting Statistics cookies. If you leave out information needed to respond to an enquiry or administer a service, we may

be unable to complete that request. We do not routinely require a date of birth, home address, passport, driving licence or NHS number for an ordinary business enquiry or contract signature.

3. Why we use information and our lawful bases

Our bases under the UK General Data Protection Regulation (UK GDPR) are set out below. Before relying on legitimate interests, we consider their effect on the people concerned.

Answering business enquiries and arranging demonstrations. We use contact details, practice details and correspondence to respond, understand the requested service and follow up the enquiry. Our basis is our legitimate interest in responding to people who contact our business and developing relevant business relationships. Where you are personally entering a contract with us, necessary steps you ask us to take before that contract can instead rely on contractual necessity. An enquiry does not subscribe you to unrelated marketing.

Providing and administering client services. We use client contact, onboarding, contract and service administration information to set up and support the agreed service and communicate with authorised practice representatives. Our basis for a company's staff contacts is our legitimate interest in managing that business relationship. Where the individual is themselves the contracting party, we rely on contractual necessity for information needed to perform that contract.

Operating the public demonstration. We use ordinary personal information deliberately supplied for a test, including an email address used to request a test confirmation, to run that demonstration, inspect its operation and investigate faults. Our basis is our legitimate interest in providing a working demonstration and checking its reliability. Real health information is not needed for that purpose; section 4 explains the limits on test data.

Delivering, securing and supporting the website. We use technical requests, error information and relevant support records to load pages and fonts, prevent misuse, diagnose problems and protect our systems. Our basis is our legitimate interest in running a reliable and secure website and service. This does not authorise optional tracking that requires a separate choice.

Measuring website use. We use Google Analytics to understand visits and interactions and improve the public website. Our basis for this optional analytics processing is your consent. You can withdraw Statistics consent through Cookiebot's settings. Withdrawal does not make earlier processing based on valid consent unlawful.

Recording privacy choices and complying with the law. We keep the information needed to demonstrate consent, deal with data protection rights and complaints, and meet accounting or other applicable legal duties. Our basis is compliance with a legal obligation. We use relevant records to establish, exercise or defend legal claims where necessary on the basis of our legitimate interests in protecting legal rights.

We do not sell personal information. We do not treat use of the demonstration, submission of an enquiry or acceptance of cookies as agreement to receive promotional emails. If we invite you to join a marketing list, the invitation will explain the separate choice and how to stop those messages.

4. Using the public chatbot demonstration

The public demonstration is for evaluating TheDentalBot. Use fictional names, telephone numbers, dental symptoms, reviews, complaints and other example details that do not identify a real person. To test a confirmation email, you may use an email address that belongs to you and that you are entitled to use. Do not enter somebody else's contact details or a genuine patient record.

Demonstration messages are not private from our business. They can be recorded in Voiceflow, passed to its integrated AI model provider to generate a response, and reviewed by us for the purposes described above. A workflow may also store structured test information in our demonstration Airtable

base and send a test email through our Resend account to the configured recipient or the address you supply. The demonstration does not require you to create an account.

A simulated appointment request, complaint or urgent enquiry in the demonstration is a test record. It is not a request for care to a real dental practice, a confirmed appointment or a live conversation with a receptionist. Do not use the demonstration to seek urgent help or disclose real clinical details.

Health information has additional protection under data protection law. We do not ask for real health information for our own demonstration and do not rely on a dental practice's healthcare condition to use it. If we discover unnecessary sensitive information in a demonstration record, we will restrict further use and arrange its deletion or removal from the test material unless a specific legal requirement or valid legal claims ground requires a restricted record to be retained. Simply entering such information or accepting this policy is not explicit consent.

To ask about a demonstration record, email enquiries@thedentalbot.co.uk. Give the approximate date and time of the chat and the email address used, if any. A session identifier can help if you have it. Please do not send additional clinical details to identify the record. We may ask for proportionate evidence that you are entitled to make the request.

5. Information processed for dental practices

In a live practice deployment, Voiceflow processes the conversation and the practice may receive structured enquiry details in its own Airtable base and email system. We use our Resend account with an authorised practice sender to deliver relevant enquiry information. We do not normally email a complete raw transcript.

Enquiry information can include a name, email address, telephone number, treatment interest, the reason for contacting the practice and the information entered during the conversation. An age band may be used where needed for child safety safeguards. A dental enquiry can reveal health information, including symptoms. The practice is responsible for identifying its lawful basis and, for health information, the additional special category condition that applies. Its privacy notice should explain these.

We can access Voiceflow transcripts where necessary to operate, support, troubleshoot, secure and check that practice's service. An integration may require us to hold a restricted Airtable access token. That does not mean we routinely read the practice's Airtable records or email inbox.

We use identifiable patient information only for that practice's agreed service and documented instructions. We do not use one practice's identifiable patient conversations for advertising, unrelated product development or improving another practice's service. Information used more widely must be genuinely anonymised so that people can no longer reasonably be identified. Removing a name alone is not necessarily enough.

For a request about a patient interaction, contact the relevant dental practice first so it can locate the record and decide the response. If a request reaches us, we will help identify the responsible practice and support it under our Data Processing Agreement. This does not prevent you from contacting us about our own handling of information.

6. Who receives information

We share information only as needed for the relevant purpose. Providers processing information for us are subject to appropriate contractual requirements. The principal services and their roles are:

Netlify: hosting and delivering the public website, with associated technical requests and operational or security information.

Supabase: processing submissions sent by the current website enquiry form. Supabase is also the planned platform for client account access and reporting. The portal remains under development; planned portal functions are not a statement that client access is already available.

Voiceflow and its integrated AI provider: operating the chatbot, generating responses and storing transcripts. The current AI processing route uses OpenAI through Voiceflow. Relevant conversation content can pass through that route. Model processing and Voiceflow's retained transcripts are separate parts of the service; a model provider's retention arrangements do not mean that the transcript has been deleted from Voiceflow.

Airtable: storing structured demonstration submissions in our demonstration base and, for live deployments, storing enquiries in the participating practice's own base.

Resend and the recipient's email provider: transmitting and receiving enquiry or test messages, with message content, addressing and delivery information. Resend is used through our account. A recipient's retained mailbox copy is separate from Resend's delivery records.

Cookiebot, provided by Usercentrics: displaying cookie choices, storing those choices and recording consent evidence.

Google: website usage measurement through Google Analytics when Statistics consent is given, and delivery of the externally hosted fonts requested by the website. We also use Search Console to review our site's visibility in Google search; this does not require visitors to accept an additional Search Console cookie on our site.

Authorised people working for us may see information needed for their role. Professional advisers, insurers, regulators, courts or law enforcement bodies may receive relevant information where necessary for advice, a legal obligation or a legal claim. We do not give a prospective client routine access to another practice's patient information.

7. International processing

Some providers and their support or infrastructure suppliers operate outside the United Kingdom, including in the United States, Canada and the European Economic Area. Information can therefore be processed outside the UK even though our business serves UK dental practices.

The planned client portal's Supabase project has its primary database in London, region eu-west-2. That location does not mean that every support or operational activity takes place only in the UK, and it is not a statement about the location of every separate website service. Voiceflow describes processing in Canada and other countries, and Resend processes customer data in the United States.

For restricted transfers, we rely on an applicable UK adequacy arrangement or appropriate safeguards, such as the UK International Data Transfer Agreement or UK Addendum to the European Commission's Standard Contractual Clauses, with any required assessment and additional measures. Adequacy arrangements apply only where their conditions and the recipient's eligibility are met.

You can contact enquiries@thedentalbot.co.uk for further information about the safeguards relevant to your information or a copy of the applicable transfer provisions, subject to proportionate redaction of confidential information.

8. Retention and deletion

The following periods distinguish our records, provider records and practice records. Deleting browser storage does not delete information held in those systems.

Business enquiries. We keep the information needed while responding and completing the associated follow up. Where an outcome or correspondence must be kept as an administrative or support record,

the period is up to 12 months after the matter is closed. If an enquiry becomes a client relationship, relevant information becomes part of the client administration or contract record instead.

Contracts and billing. We retain records needed during the relationship and afterwards for applicable record keeping duties or legal claims. Company accounting records are normally kept for six years from the end of the financial year to which they relate, with longer retention where the law requires it. Relevant agreement and dispute records are kept for the period needed to establish, exercise or defend the particular legal rights, taking account of applicable limitation periods and any ongoing proceedings.

Voiceflow transcripts. Identifiable chatbot transcripts may currently be retained for up to six months under the service configuration. Where a live practice's service ends, we initiate provider deletion without undue delay, subject to completing any agreed return first. Necessary records relating to a specific incident or legal obligation are assessed separately and access is restricted.

Connected demonstration records. A structured Airtable record or a received test email is a separate copy from the Voiceflow transcript. There is currently no single automatic deletion period applying to all of those demonstration copies. We assess whether the identifying details are still needed for the particular test, unresolved fault, support request or legal issue. Records are deleted or anonymised when that purpose ends; retaining an identifiable record merely because it might be useful for unspecified future development is not our retention criterion. You can request deletion using the contact details in section 4.

Resend delivery records. Resend's published retention for its Free, Pro and Scale plans is 30 days for email and log data, with backups retained for seven days. Its stated period for deleting remaining customer data after account termination is 90 days. Account termination here means closure of our Resend account, not cancellation by one dental practice. Copies already delivered to a mailbox are governed by that mailbox's controller.

Support, security and administration. Relevant records may be retained for up to 12 months where reasonably necessary for support, investigation, security or administration. This does not justify routinely copying full patient transcripts into support files. If a particular legal duty or claim requires a longer period, we retain only the relevant information for that purpose.

Consent evidence. Cookiebot retains its identifiable consent log for 12 months under its published terms. A record needed to deal with a particular complaint or demonstrate compliance may be retained separately for as long as that matter requires. The browser cookie's lifetime is a different period and is described in the Cookies Policy.

Website analytics. Google Analytics applies its property retention settings to user and event data. In a standard GA4 property the available periods are two or 14 months; a user identifier's period can be renewed by further activity if that setting is enabled. Those controls do not apply in the same way to standard aggregated reports. The cookie expiry shown in our Cookies Policy is not the analytics record retention period. Contact us for the current property setting applicable to your visit.

Practice and future portal records. The practice sets retention for its own Airtable, CRM and mailbox records. Return or deletion of data held for it follows its instructions and our Data Processing Agreement. At service end, planned Supabase account and reporting data will enter the agreed deletion process, subject to completing a return and applicable legal retention. Ending access does not remove the return right.

Deletion from active systems may precede expiry from provider backups. Information awaiting deletion or backup expiry is kept beyond ordinary use; deletion instructions must be reapplied if a backup is restored. Genuinely anonymous statistics may be kept for longer because they no longer identify an individual.

9. Security, children and automated processing

We use access restrictions and technical and organisational measures appropriate to the information and service, and limit access to people who need it for their role. No internet service can promise absolute security. Please avoid sending unnecessary sensitive information and tell us promptly if you believe information has been exposed or sent to the wrong recipient.

The public business website and demonstration are intended for people evaluating services for a dental practice. They are not intended to collect children's personal information. If you believe a child has supplied such information in the demonstration, contact us so we can investigate and remove information that should not be held. For a child using a real practice's chatbot, the practice remains responsible for the applicable patient privacy information and any parental involvement or clinical consent requirements.

The chatbot generates automated responses and can organise an enquiry for human follow up. It is not intended to make solely automated decisions about you with legal or similarly significant effects. It does not replace a dentist's diagnosis or treatment decision. Submission of an enquiry does not itself confirm an appointment or treatment.

10. Your rights and choices

Depending on the circumstances, you can ask for access to your personal information and a copy of it, correction of inaccurate information, erasure, restriction of use, or transfer of information you supplied where the right to data portability applies. You can object to processing based on legitimate interests. You have an absolute right to object to use of your information for direct marketing.

Where we rely on consent, you can withdraw it at any time. For Statistics cookies, use Cookiebot's settings. For another consent based activity, use the contact or withdrawal method given when consent was requested. Rights are subject to the conditions and exceptions in law; for example, we may need to keep an accounting record even after an erasure request.

Send requests to enquiries@thedentalbot.co.uk or our registered office. We normally respond within one month, subject to the identity, clarification, extension and other rules permitted by applicable law. We will explain any permitted extension or reason why a request cannot be met. Requests are normally free. We ask only for information reasonably needed to verify entitlement and locate the record.

Where the information belongs to a practice's patient workflow, section 5 explains how to direct the request. You do not need to accept optional cookies or complete a marketing form to exercise a data protection right.

11. Complaints and changes to this policy

If you are concerned about our handling of personal information, email enquiries@thedentalbot.co.uk or write to our registered office. Describe the concern and how you would like us to contact you. We will acknowledge a data protection complaint within 30 days, investigate without undue delay, keep you appropriately informed and explain the outcome.

You can complain to the Information Commissioner's Office (ICO), the UK data protection regulator, including if you are dissatisfied with our response. Information is available at ico.org.uk/make-a-complaint/ or on 0303 123 1113. You do not lose this right by contacting us first.

We will update this policy when relevant purposes, systems, recipients or legal requirements change. For material changes affecting your information, we will provide appropriate notice and obtain a new choice where required.