

Privacy Policy

Website enquiries and business relationships

1.0 Identity and scope

1.1 Sun Tech Precision is a partnership firm with GSTIN 29ADKFS1829A1Z3, located at #685, 5 & 6, Tigalarapalya Main Road, Near New Indian National High School, Peenya 2nd Stage, Bengaluru, Karnataka - 560058, India. Our website is <https://suntechprecision.com>. This Privacy Policy is effective from 09 October 2026 and explains how we handle personal information connected with our website, contact enquiries, WhatsApp communications and business relationships. "We", "our" and "STP" refer to Sun Tech Precision; "you" refers to an individual whose personal information we process.

1.2 The policy covers visitors, customer and supplier representatives, applicants, employees, contractors and premises visitors where relevant to their interaction with us. Specific employment, CCTV, attendance, visitor or recruitment notices supplement this policy. Confidential drawings and commercial records also remain subject to applicable confidentiality and contractual obligations even where they do not contain personal data.

2.0 Information collected through the website

2.1 Our website provides contact enquiries and access to WhatsApp chat. Information you choose to submit may include your name, organization, email address, contact number if voluntarily supplied, enquiry content and related correspondence. Please provide only information needed for your request and avoid unnecessary identification documents, financial credentials, health information or information about other people.

2.2 Technical information generated in operating the website may include IP address, browser and device information, access time, requested page and security-event records. Such information is used for reliable operation, troubleshooting, abuse prevention and security. We do not treat the existence of a browser connection as permission for unrelated advertising or profiling.

2.3 The website is not an online payment, customer-account, job-application or document-upload portal. A contact enquiry does not create an account, subscribe you to a newsletter or authorize recurring promotional communications. If further information is required to respond to an enquiry, we will request it through an appropriate business channel.

3.0 WhatsApp communications and external services

3.1 When you choose WhatsApp chat, WhatsApp processes information under its own terms and privacy policy. Depending on your settings and interaction, we may receive your profile name, contact number, message content and attachments. You may instead contact us by email at sales@suntechprecision.com. Using WhatsApp is optional and is not a condition for receiving a response to an ordinary business enquiry.

3.2 We use messages to respond to your enquiry, maintain necessary correspondence and progress the requested business interaction. Do not send export-controlled technical data, passwords, identity documents or highly sensitive material through WhatsApp unless a suitable secure process has been agreed. WhatsApp's handling of data, hosting and account metadata is not controlled solely by STP.

4.0 Business employment and premises information

4.1 For customers and suppliers, we may process professional contact details, role and organization, correspondence, order and delivery information, payment-related records and compliance documentation necessary for the relationship. Information relating only to a legal entity is distinguished from information identifying an individual, including sole proprietors and individual signatories.

4.2 For applicants, employees and contractors, we may process applications received outside the website, qualifications, employment history, identity and statutory records, attendance, payroll, emergency contacts and benefits information as required for recruitment or administration. Access to health, financial and identity information is restricted according to need, and collection through informal public enquiry channels is discouraged.

4.3 Where CCTV or biometric attendance is used, a specific notice shall identify the purpose and appropriate contact. CCTV shall be limited to legitimate security and incident-management purposes and shall not be installed in areas where privacy is reasonably expected, such as toilets or changing rooms. Biometric information shall not be repurposed for publicity or unrelated profiling; necessary verification, security and lawful alternatives shall be considered in administering attendance.

5.0 Purposes and lawful processing

5.1 We process necessary information to answer enquiries, discuss machining capabilities, assess requirements, manage quotations and orders through agreed channels, administer suppliers, fulfil employment duties, protect premises and systems, investigate concerns and comply with law. We identify a lawful basis for each activity and limit use to compatible, disclosed purposes.

5.2 Where consent is required, we seek a clear affirmative choice after providing relevant information. Where a permitted use under applicable law is relied on, such as specified voluntarily supplied information or employment-related processing, we assess and document the conditions for that use. A general business interest is not treated as an unrestricted legal basis under the DPDP framework.

5.3 Optional publicity, testimonials or promotional contact require an appropriate separate permission where applicable. We do not sell personal information or permit service providers to use information received on our behalf for their own unrelated marketing. A change to a materially different purpose requires a fresh legal assessment and any necessary notice or consent.

6.0 Choices and consent withdrawal

6.1 You may decline optional information and may withdraw consent by contacting the Managing Partner at sales@suntechprecision.com with the subject "Privacy Request". Withdrawing consent shall be as straightforward as giving it. We will stop the affected consent-based activity and direct relevant processors to do so within a reasonable period, unless continued processing is required or authorized by applicable law.

6.2 Withdrawal does not invalidate processing lawfully completed before withdrawal. If particular information is necessary to answer an enquiry, complete a requested service or meet a legal obligation, we will explain the relevant consequence of not providing it. Optional marketing or publicity choices shall not be bundled with necessary business processing.

7.0 Cookies and similar technologies

7.1 Essential website functions and security mechanisms may use cookies or similar technical storage where deployed. The site shall not activate optional advertising or analytics trackers without the required notice and choice. Introducing new tracking tools requires a review of their purposes, providers, information collected, retention and consent requirements before activation.

7.2 You may manage browser storage through your browser settings. Disabling necessary storage may affect specific functions. Links or buttons that open WhatsApp or other external services may involve that service's own technologies after you choose to use them. We do not represent that third-party services are governed exclusively by this policy.

8.0 Disclosure and service providers

8.1 We share information only with authorized personnel and recipients who need it for a disclosed purpose, including relevant customers or suppliers, hosting and IT support providers, professional advisers, payroll or statutory-service providers, and logistics providers where needed for the transaction. Recipients receive the minimum information reasonably required, subject to applicable confidentiality and security arrangements.

8.2 Processors acting for STP shall be engaged under written terms restricting use to authorized instructions, requiring appropriate security and governing sub-processors, incidents, rights assistance and return or deletion. Disclosures to independent entities, such as banks or statutory authorities, shall be assessed separately according to their role and legal basis.

8.3 We may disclose necessary information in response to a lawful obligation, enforceable request, legal proceeding or genuine need to establish or defend rights. We assess the request, limit disclosure and preserve a record. Any business restructuring involving information shall be subject to applicable law, suitable safeguards and required notices; this clause does not authorize unrestricted transfer.

9.0 International transfers

9.1 Personal information may be processed outside India where a selected communication or service provider uses overseas infrastructure. Before authorizing an international transfer, we assess the destination, recipient, purpose, security arrangements and restrictions applicable to that information. Consent, where relevant, does not override a statutory transfer prohibition.

9.2 Transfers shall comply with applicable Indian restrictions and any binding sector-specific requirement. The DPDP framework does not create a universal prohibition on all overseas processing; applicable government notifications and orders shall be observed as they take effect. Restricted customer or defence information shall be subject to any additional contractual or export-control limitations.

10.0 Retention and deletion

10.1 Information is retained only for the relevant purpose and applicable legal requirements, with controlled review of retention. Enquiry records that do not progress into a business relationship are reviewed for deletion within 12 months after closure. A longer period requires a documented reason such as an active dispute, legal obligation or continuing request; merely keeping data for possible future use is insufficient.

10.2 Order, financial, employment and quality records follow applicable statutory and contractual schedules. Supplier quality records may require ten years or a longer specified period; that period does not automatically apply to all personal information. Personal identifiers within long-retained technical records shall be minimized, access restricted and retention justified under applicable law.

10.3 Where operative DPDP Rules require retention of specified personal data, associated traffic information or processing logs for at least one year, the applicable records shall be preserved accordingly. Security-log retention under other applicable rules shall also be observed. Erasure requests and routine deletion shall account for legal holds and these requirements, with a reason provided where immediate deletion is not permissible.

10.4 Deletion shall cover active systems and relevant processors, with backups isolated from ordinary use and removed under controlled backup cycles. Paper records shall be securely destroyed and electronic information deleted or irreversibly anonymized where appropriate. Deleted records shall not be restored for unrelated routine processing.

11.0 Security and incident handling

11.1 We require reasonable administrative, technical and physical safeguards appropriate to the information, including access restrictions, secure transfer, suitable encryption or masking, authentication, system maintenance, backups and incident escalation. Access is limited to authorized personnel, and confidentiality obligations continue after their engagement ends.

11.2 If a personal-data incident occurs, we assess its nature, contain it, preserve evidence and take corrective action. Affected individuals and competent authorities shall be notified where required under the law and within applicable timelines. No communication method or system is entirely immune to compromise; this does not reduce our duty to maintain reasonable safeguards or meet mandatory incident-reporting obligations.

12.0 Requests access correction erasure and nomination

12.1 You may contact us to seek access to information concerning our processing, correction of inaccurate information, completion or updating of records, erasure where permissible, consent withdrawal, or grievance redressal. Rights under the DPDP Act, including nomination of another individual for exercise of rights upon death or incapacity, apply in accordance with their statutory scope and commencement. STP will also consider reasonable privacy requests under this policy during the transition.

12.2 Requests should identify your relationship with us, the relevant email or other reference and the action requested. We use proportionate identity verification and will not routinely demand a full identity document when a less intrusive check is adequate. We protect third-party information and confidential records when responding, explain lawful limitations and retain a minimal record of the outcome.

13.0 Children and supported decision making

13.1 Our website and machining services are directed to business users and are not intended to solicit information from children. Please do not submit a child's information through the general enquiry channel. Where lawful employment-benefit, emergency or other permitted processing involves a child, the required parent or lawful guardian verification and specific safeguards shall be applied.

13.2 Where a person with a disability has a lawful guardian and applicable law requires guardian consent, we verify the authority and obtain the required consent. Disability alone is not treated as proof that a person cannot make decisions or exercise their rights.

14.0 Grievance contact and escalation

14.1 Requests shall be addressed to the Managing Partner, Sun Tech Precision, at sales@suntechprecision.com, or by post to #685, 5 & 6, Tigalarapalya Main Road, Near New Indian National High School, Peenya 2nd Stage, Bengaluru, Karnataka - 560058, India. Please use the subject "Privacy Grievance" and provide enough information to identify the matter without sending unnecessary sensitive documents.

14.2 We aim to acknowledge a grievance within seven working days and resolve it within 30 calendar days of receipt, subject to any shorter mandatory period. Where additional verification is necessary, we will explain the next steps and will not use verification to defeat a statutory deadline. A person dissatisfied with our response may pursue the competent statutory authority or forum available under

applicable law, including the Data Protection Board of India when the relevant provisions and complaint mechanism apply. Mandatory prior grievance steps shall be observed.

15.0 Applicable law policy changes and jurisdiction

15.1 This policy shall be interpreted under Indian law, including applicable provisions of the Information Technology Act and rules, the Digital Personal Data Protection Act, 2023, and Digital Personal Data Protection Rules, 2025 as brought into force. A future statutory obligation applies from its notified commencement, while commitments expressly adopted in this policy apply from its effective date to the extent lawful.

15.2 Material changes will be published with a revised effective date, and additional notice or consent will be provided where required. Changes do not retrospectively authorize a use that was unlawful when undertaken. Courts of competent jurisdiction at Bengaluru, Karnataka, India shall have jurisdiction over matters lawfully subject to that choice; statutory regulators, appellate bodies and other non-excludable remedies remain unaffected.