

SOUL Privacy Policy

CUSTOMER AND VISITOR PRIVACY NOTICE

Bookings | SOULcare | SOULrecharge | Website and communications

Controller	SOUL Wellness C.I.C., trading as SOUL Wellness Hub & Cafe
Company number	15059642
Address	The Former Methodist Church, Burnley Road, Sowerby Bridge, West Yorkshire, HX6 2TL
Privacy contact	SOUL management info@soulwellnesshub.com
Effective date	11 September 2026

This policy explains how SOUL uses and protects personal information when you book, visit, become a member or use our website. It explains your choices and how to contact SOUL management about your information. It is separate from our booking and cancellation terms.

1. Who we are and how to contact us

SOUL Wellness C.I.C. ("SOUL", "we", "us" or "our") is the controller of personal information used to run our business and provide our own services. A controller decides why and how personal information is used. Please email SOUL management at info@soulwellnesshub.com for privacy enquiries or requests. You may also write to the address above. No particular form is required.

This notice explains our handling of personal information under the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations, as amended. It is information about our practices, not a request for blanket consent and not a waiver of your rights.

2. Who and what this notice covers

It covers customers, SOULcare members, SOULrecharge guests, website visitors, people making enquiries or receiving our marketing, and individuals booking on someone else's behalf. It also covers personal information about room hirers, independent practitioners and other business contacts when dealing with SOUL.

Services include our float tank, infrared sauna, hot tub, ice bath, Amethyst Room, spa-day packages, memberships, SOUL-run classes and events, cafe services and room hire. Separate privacy notices may apply to staff, recruitment or a particular event. Independent practitioners may be controllers of their own consultation and treatment records; see section 9.

Our website is soulwellnesshub.com. Third-party websites and platforms have their own privacy information. Our General Terms, membership and service terms explain bookings, payments and cancellation rights; this notice explains personal-data use. Accepting those terms does not automatically provide marketing or health-data consent.

3. Personal information we collect

We collect information relevant to the relationship or service, not every category for every person. We identify required booking fields; without necessary contact, eligibility or payment information we may be unable to accept or fulfil the booking. Optional preferences and marketing choices are not required. Please do not send medical histories, identity documents or card details unless specifically requested through an appropriate channel.

Identity and contact details: name, email, telephone number, postal or billing address, and age or date of birth where reasonably needed to check eligibility. We may record the identity or authority of a parent, guardian or representative.

Bookings and membership: selected services, dates, attendance, cancellations, account credits, vouchers, membership plan and status, benefit usage, preferences, package arrangements and communications about your booking.

Payments and accounts: amounts paid, billing information, transaction references, payment status, refunds, recurring-payment records and disputes. Payment services may provide limited card information such as brand and last four digits. Please do not email us your full card number or security code.

Health and safety: relevant screening answers, allergies, pregnancy, medication, medical conditions, accessibility needs, contraindications and information about an accident or adverse reaction. Dietary information can reveal health or religious information. We limit collection to what is necessary and apply the extra safeguards in section 6.

Communications and preferences: enquiries, feedback, complaints, consent records, marketing choices and correspondence. Where agreed, this may include photographs, testimonials or event recordings. Marketing delivery and interaction information is addressed in section 11.

Website and security: IP address and technical request data, browser and device details, pages viewed, approximate location derived from technical data, referral information and cookie or similar identifiers, depending on your choices and the tools in use. CCTV can capture images and the time and location of a visit; see section 13.

Professional contacts: contact details, invoices, room bookings and relevant qualifications or insurance evidence for practitioners and hirers. We do not need their complete client records merely because they hire a room.

4. Where information comes from

Most information comes from you when you book, join, visit, complete a screening form, pay, contact us or choose to subscribe. It can also come from someone arranging your booking, a parent or authorised representative, payment and booking providers, a practitioner involved in your package, or an incident witness. Website tools and CCTV collect information as described in this notice.

If someone books for you, we normally receive only the details needed to arrange attendance. They should tell you they have shared your information and give you this notice. We seek sensitive screening information directly from the person concerned where practicable. Where information comes from another source, we provide the required privacy information within the applicable legal timescale, normally within one month or sooner at first contact or disclosure.

5. Why we use information and our legal bases

We identify a lawful basis for each purpose. The same record can be used for more than one distinct purpose, but we do not treat the bases below as interchangeable. "Legitimate interests" means a necessary, proportionate business or safety purpose balanced against your rights and reasonable expectations.

Bookings, membership and payment administration: contact details, booking records, plan usage and transaction information are used to arrange and deliver services, take recurring payments, send service messages, and process changes, credits and refunds. Our basis is performance of our contract with you, or steps you ask us to take before a contract. For an attendee who is not the contracting customer, our basis is our legitimate interest in administering the booking and providing the requested service.

Enquiries and business relationships: we use correspondence and professional-contact information to respond, arrange room hire and manage suppliers or practitioners. We rely on contractual necessity where you are a party to the contract; otherwise, our legitimate interests in responding and managing those relationships.

Accounting and legal compliance: we use necessary transaction and business records to meet tax, accounting and applicable statutory reporting duties. Our basis is legal obligation. Where a specific reporting duty applies to an incident, we use only the information required for that duty.

Safety, security and disputes: we use relevant attendance, communication, incident and security records to protect people and property, prevent fraud, investigate complaints and establish or defend legal claims. Our basis is legitimate interests in those purposes, or legal obligation where a specific duty applies. Health information also needs the condition explained below.

Optional marketing, analytics and publicity: we rely on consent for optional analytics and identifiable promotional photographs or testimonials. For email marketing, we rely on consent, or legitimate interests where the existing-customer marketing exception lawfully applies. That exception has additional requirements explained in section 11. Essential service messages do not depend on marketing consent.

6. Health information and sensitive data

For routine safety screening needed to provide your requested wellness service, we rely on contractual necessity (or the attendee-related legitimate interest above) and your explicit consent under Article 9(2)(a) UK GDPR. We request that consent separately, explaining the information, purpose, necessary recipients and withdrawal route. A signature accepting general terms is not enough. We do not assume that ordinary wellness services qualify for the medical-treatment exemption.

You may refuse or withdraw explicit consent by contacting us. This does not make earlier lawful processing unlawful. If the information is genuinely necessary to assess safe participation, we may be unable to provide the affected service; we will explain why and consider reasonable alternatives. Refunds remain governed by applicable terms and consumer law, not by a blanket privacy-consent penalty.

In a genuine emergency, necessary processing to protect life may rely on vital interests under Article 6(1)(d). For health data, Article 9(2)(c) applies only where the person is physically or legally incapable of giving consent. Necessary processing for legal claims may rely on Article 9(2)(f), alongside an appropriate Article 6 basis. These are not general exceptions for routine screening.

SOUL keeps paper health screening forms in a locked cupboard, with access limited to those who need the information for their work. Forms are normally completed once per customer and retained for 12 months. Please tell us before a later visit if relevant health information has changed; a previous form does not replace an up-to-date safety assessment. We do not currently add these forms to a digital system. We will explain any material change before introducing electronic health records. Health information is not used for marketing audiences or analytics.

7. People under 18 and bookings for others

Service-specific age restrictions apply. We collect only the age, guardian, booking and safety information needed for an eligible young person. Privacy information must be understandable to them. Capacity to consent depends on their understanding and the circumstances, not booking permission alone. We verify a representative's authority before disclosure.

8. Who receives information and our platforms

We share only what is needed for the stated purpose, with access according to authorised roles. Using one service does not mean every platform receives all your information.

Koalendar: booking and scheduling details, such as name, contact information, appointment and relevant booking answers, to arrange and manage appointments. Stripe: billing and transaction information to process payments, recurring charges, refunds and payment disputes. Stripe also processes some information for its own fraud-prevention and legal-compliance purposes; its role depends on the activity. See stripe.com/gb/privacy.

Google Sheets: we use our business Google account to maintain operational records including names, mobile numbers, email addresses and subscribed packages, and records of voucher purchasers. Front-of-house staff can access information needed for their work. Zapier connects selected booking and administration systems and transfers information needed for those workflows; its processing may include workflow histories. Our paper screening forms are not currently entered into these systems.

Brevo, formerly Sendinblue, manages our mailing list and emails, including subscription, delivery, open and click information. Google Analytics measures website use. Our WordPress website is hosted by Bluehost and uses WPForms Lite for contact forms. Submitted enquiries and technical information are handled as needed to deliver and protect these services.

Website features may involve additional providers when used: Jetpack and AIOs for site operation and security; UpdraftPlus for backups; OptinMonster for signup features; Styled Calendar and Google Reviews widgets for embedded content; and Ticket Tailor for event booking. MonsterInsights and Site Kit connect website features with Google services. The information involved depends on the enabled feature and your interaction, not simply whether a plugin is installed. Necessary recipients can also include accountants, professional advisers, insurers, IT providers, banks, emergency services, regulators and courts where disclosure is necessary and lawful.

Suppliers acting as processors are required to process information under our instructions and appropriate data-protection terms. Some providers, such as payment providers for their own compliance activities, act as separate controllers and provide their own privacy notices. We do not sell customer lists or share them for other organisations' marketing.

9. Independent practitioners and SOULrecharge

SOUL uses booking and scheduling information to arrange SOULrecharge packages. Our employed therapists do not keep separate treatment records. Independent therapists who hire a room may hold their own consultation or treatment records under a separate relationship with their customer. SOUL shares the customer's name for arrangements where needed, but does not routinely provide those therapists with our screening forms or clinical information.

Independent practitioners are responsible for explaining their own record keeping, lawful bases and privacy rights arrangements where they control that information. Room hire alone does not make SOUL the controller of their treatment records. Any information SOUL itself holds remains our responsibility. Ask us if you are unsure who holds a particular record.

10. Information processed outside the UK

Our cloud providers and their support or subprocessor networks may process information outside the UK, including in Europe and the United States. A restricted international transfer requires a valid legal route: for example, UK adequacy regulations or appropriate contractual safeguards such as the UK International Data Transfer Agreement or the UK Addendum to EU standard contractual clauses, with any required risk assessment and additional protections. The route depends on the provider and processing involved. Contact SOUL management for details of the arrangements relevant to your information and how to obtain a copy of applicable safeguards, subject to necessary redactions.

11. Email marketing and your choices

We use Brevo for email marketing. Contacts enter our mailing list through direct signups and our digital booking, purchase and subscription workflows. Being added to a contact list is not, by itself, consent to receive promotional emails. Marketing is permitted only where we have valid consent or every condition of the applicable existing-customer exception is met.

You can unsubscribe using the link in a marketing email or contact us at info@soulwellnesshub.com. You can stop one marketing channel without cancelling your membership or bookings. We retain a minimal suppression record where necessary to honour your choice. Essential booking confirmations, safety notices, payment messages and important membership administration can still be sent.

For the existing-customer exception, we must obtain your contact details directly during a sale or negotiations for a sale, market only our own similar products or services, and give you a clear, simple opportunity to refuse marketing when details are collected and in every subsequent message. A purchase, a privacy-policy acknowledgement or an unsubscribe link alone does not satisfy all these conditions. Where we rely on this exception, our legitimate interest is promoting relevant services to existing or prospective customers within those limits.

Brevo tracks email opens and link clicks using email technologies and records engagement to help us assess communications. This may involve identifiers and technical information; an open signal is not always a reliable indication that you read a message. Any consent required for these tracking technologies is separate from permission to send marketing. Contact us about tracking or unsubscribe to stop future promotional emails. We do not currently create interest-based customer groups or use health screening answers for marketing.

12. Website, Google Analytics and cookies

Our WordPress website uses technical information to operate and protect the site, handle forms and support bookings. Strictly necessary cookies or similar technologies may be used without consent where the legal exemption applies. We rely on legitimate interests in operating a secure site, or contractual necessity for a requested booking function, as appropriate.

We use Google Analytics to understand visits and interactions and improve our website. Depending on configuration, this involves browser and device details, identifiers, referral pages, approximate location and events such as page views and clicks. Information is not necessarily anonymous merely because it does not include a name. Names, email addresses and health answers should not be sent in analytics events or page addresses.

Optional analytics and other non-essential storage or access technologies require your prior consent unless a specific legal exception applies. Rejecting optional analytics should not prevent ordinary browsing or booking. Cookie-free tracking can still involve personal information. Browser settings can block or remove cookies, although this may affect some functions and does not necessarily stop every form of tracking. Contact us with questions about website privacy choices.

Embedded calendars, reviews, signup tools and event checkout features may connect to third-party services when loaded or used. Their technical data and storage behaviour depend on the feature. Any cookie notice or consent interface provided with those features should be read alongside this policy. This policy does not itself record cookie consent.

13. CCTV, photographs and recordings

CCTV operates in designated customer-facing and external areas for safety, security and incident investigation. Our lawful basis is our legitimate interests in protecting people and property and investigating incidents. Signs identify monitored areas. CCTV records images and times, not sound. Footage is stored locally and only SOUL directors are authorised to view it. Routine recordings are overwritten every seven days; incident extracts may be retained for up to 12 months. We do not publish camera layouts or security blind spots.

We disclose footage only where necessary and lawful, for example to police, insurers or advisers dealing with an incident or claim. Access requests may require redaction to protect other people. Where a specific legal requirement or active legal claim requires retention beyond the normal period, only the relevant material is retained for as long as necessary and subject to review.

We use identifiable promotional photographs, testimonials or recordings only with permission, explaining the intended use. Attendance alone is not permission to appear in advertising. Children do not appear in our promotional images. You can withdraw consent for future use by emailing us; earlier lawful use is unaffected. We will stop further consent-based use, although copies already distributed or independently shared by others may not be recoverable.

14. How long information is kept

We keep personal information only for as long as it is needed for its purpose. The period depends on the service relationship, sensitivity, applicable legal duties, relevant claim periods and any continuing need. Where no fixed period is stated below, these criteria determine retention rather than an indefinite entitlement to keep the information.

Bookings and membership records: keep operational information while required to manage the booking or membership. After it ends, retain only records needed for outstanding credits, refunds, complaints, legal obligations or a justified claims period. Account closure does not automatically remove invoices that must legally be kept.

Financial records: keep the records required by applicable accounting and tax rules for the relevant statutory period. The period and starting point depend on the record and circumstances. We do not retain a whole health form merely because an invoice must be retained.

Health screening and incident records: routine paper screening forms are retained for 12 months. Relevant information needed for an incident, complaint or legal claim may need separate retention while the matter remains unresolved or a justified legal need continues. Any extended use of health information also requires an appropriate special-category condition. We do not retain a complete health form solely because an invoice must be retained.

Enquiries and complaints: retain while dealing with the matter and for a justified period afterwards to address follow-up, evidence the outcome and manage legal risk. Remove unrelated or unnecessary sensitive detail.

Marketing: retain subscription details while there is a valid marketing basis and they remain relevant. Minimal consent evidence and suppression records may be retained as necessary to demonstrate and respect your choices.

Unsubscribing does not require deletion of the limited record needed to prevent further marketing.

CCTV, analytics and system histories: routine CCTV is overwritten after seven days and incident extracts are normally kept for no more than 12 months, subject to the exceptions above. Analytics, website logs, automation histories, spreadsheets and backups are retained according to their operational purpose, security needs and applicable system settings. Contact us for the current period or criteria applying to a particular record.

Information no longer needed is securely deleted, shredded or genuinely anonymised. Backup copies may remain until their overwrite cycle completes; deletion requirements must be reapplied if a backup is restored. Any legal hold is limited to relevant information and reviewed. You may ask us about the retention of your own information.

15. How we protect information

We use individual staff logins, limit access to information needed for each role and remove access when staff leave. Important accounts use two-step authentication. Paper screening forms are kept in a locked cupboard and paper records are securely shredded when disposed of. Website administration is restricted to the business owner. These measures are intended to reduce unauthorised access, loss and misuse.

No method of storage or transmission is completely secure. If a personal-data breach occurs, we investigate, contain it and make notifications to the regulator and affected people where required by law. Please report suspected loss, misdirected messages or unauthorised access promptly using our privacy contact details. Do not send sensitive details in a public review or social-media comment.

16. Your rights and how to use them

You have rights over your personal information. Their application depends on the processing, lawful basis and any legal exemptions. You can contact us by email or post; you do not need legal wording or to pay an administration fee merely to make a request.

Access and correction: ask whether we hold information about you, request a copy and relevant details about its use, or ask us to correct inaccurate or incomplete information.

Erasure and restriction: ask us to delete information where the legal conditions apply, or limit its use, for example while accuracy or an objection is considered. These rights do not require us to delete information we must lawfully retain.

Portability: where processing is automated and based on consent or a contract, ask for eligible information you provided in a structured, commonly used, machine-readable format, or for it to be transmitted to another controller where technically feasible.

Your right to object: you can object to processing based on legitimate interests for reasons relating to your circumstances. We must stop unless we demonstrate compelling overriding grounds or need the information for legal claims. You can object to direct marketing, including related profiling, at any time; we will stop that use. This marketing right is not subject to a balancing test.

Withdrawal of consent: withdraw consent at any time, as easily as it was given, without affecting earlier lawful use. Use the unsubscribe option or email us, as appropriate. Health-consent consequences are explained in section 6.

We respond without undue delay and normally within one month of the applicable starting point. Where the law permits extra time for complex or multiple requests, we explain the extension and reasons within the required timeframe; the extension can be up to two further months. We may reasonably verify identity or seek necessary clarification. We explain any lawful refusal, limitation or permitted charge and your complaint options.

Automated decisions: SOUL does not make solely automated decisions about you that have legal or similarly significant effects. We use routine booking, administration and payment automation. Payment providers may apply their own automated fraud checks; their privacy notices explain their processing and relevant rights.

17. Privacy complaints

If you are unhappy with our use of personal information, email SOUL management at info@soulwellnesshub.com or write to our address above, marked "Privacy complaint". Explain your concern and, if possible, the outcome you want. We will acknowledge a data-protection complaint within 30 days, make appropriate enquiries, keep you informed as appropriate and communicate the outcome without undue delay.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK data-protection regulator: ico.org.uk/make-a-complaint/ or 0303 123 1113. We would welcome the opportunity to resolve a concern first, but this does not remove your right to approach the ICO or seek a remedy through the courts.

18. Changes to this notice

We review this notice when our services, systems or legal obligations change. The published version will show its effective or last-updated date. We will give appropriate notice of material changes and, where required, seek fresh consent before a new consent-based use. Publishing a revised policy does not retrospectively authorise an incompatible use of your information.