CUSTOMER PRIVACY NOTICE

Privacy and Data Protection Statement

Macole's Self Catering Holidays Limited

Version 2026/001 | Review draft | 5 September 2026

In plain terms

We use personal data to answer enquiries, arrange and administer bookings, support guests, meet legal duties, protect our business and customers, and - only where permitted - send marketing. Service communications are separate from marketing. We do not sell personal data.

1. Who we are

Macole's Self Catering Holidays Limited (company registration number 28376) is the data controller responsible for deciding how and why personal data is used for the activities described in this Statement. Macole's, Macoles and Macole's Self Catering are our trading names.

Registered address: Maison Amicale, Rue De Trachy, St Helier, Jersey, JE2 3JN.

Data protection contact: administration@macoles.com | +44 (0)330 1749 320 | the postal address above.

We are primarily subject to the Data Protection (Jersey) Law 2018 (DPJL 2018). Where another regime applies to a particular activity - including the UK GDPR, the UK Data Protection Act 2018 or the Privacy and Electronic Communications Regulations (PECR) - we will also meet the applicable requirements.

2. What this Statement covers

This Statement applies when you enquire about, request or make a booking; travel as a member of a booking party; use our website, online booking, chat or communication services; contact us by telephone, email, SMS, WhatsApp, social media or post; respond to a survey or review request; or become involved in a complaint, claim or dispute.

It does not replace our contractual terms. This customer Statement does not cover recruitment or employment information; a separate privacy notice will be provided when relevant.

3. The personal data we collect

The information depends on the service requested and may include:

- Identity and party information: names, titles, ages or dates of birth, nationality, and details needed to identify the party leader and party members, including children.

- Contact information: postal address, email address, telephone or mobile number, contact preferences and emergency contact details.
- Booking and travel information: dates, accommodation preferences, party composition, booking reference, arrival and departure details, ferry or flight information, and communications with accommodation and transport providers.
- Identity and regulatory information: passport or identification details only where reasonably required for travel, immigration, fraud prevention, legal or supplier requirements. We seek to record the minimum necessary rather than retaining complete documents.
- Payment and transaction information: payment status, amount, method, transaction identifiers, refunds, bank details where needed, and limited payment-card information supplied by payment providers. We do not normally store full card numbers or security codes.
- Special requests and preferences: accessibility, dietary, religious or other requirements. These can reveal special category data, such as health, disability or religious belief, even if you do not provide a diagnosis. We do not record or store such information and prefer that you provide the needs required without disclosing any other information, as it is not relevant to our function.
- Communications and service records: emails, messages, chat transcripts, call details, call recordings where used, notes, complaints, feedback, reviews and evidence connected with the booking.
- Technical and usage information: IP address, cookie or visitor identifiers, approximate location derived from IP, date and time, pages or links used, referring source, browser, operating system, device type, security logs and interaction with our digital services.
- Email-event information: delivery, bounce and complaint events and, where tracking is enabled and permitted, whether an email appears to have been opened, links selected, time, IP address, approximate location and device or browser information.
- Marketing information: preferences, consent records, unsubscribe or objection records, campaign history, and inferred interests based on lawful and transparent interaction data.

MAC addresses and other device identifiers

A hardware Media Access Control (MAC) address is not normally transmitted to us when a person visits a public website or reads an email. We do not seek to collect a device's MAC address through ordinary website or email activity. If a local network or a future service makes a MAC address or another persistent device identifier available, we will assess the need, explain the processing and apply the requirements in section 15 before using it.

4. Where personal data comes from

We collect data directly from you and indirectly from the party leader, another party member or authorised representative; an accommodation owner, manager or provider; a carrier or travel supplier; a payment provider or bank; an insurer, adviser, regulator or public authority; our website, cookies, email, telephony and chat systems; and publicly available sources where necessary and lawful.

If you provide information about another person, you must have authority to do so and should give them access to this Statement. We may also provide the Statement directly to a party member where required by law, practical and appropriate.

5. How and why we use personal data

We only process personal data where we have a proper reason under the DPJL 2018. Consent is not used as a blanket basis for administering a booking. The principal purposes and lawful bases are:

Purpose	Lawful basis and explanation
Enquiries, quotations and requested proposals	Steps requested before entering a contract; and legitimate interests in responding efficiently and keeping an enquiry record.
Create, confirm and administer bookings; arrange accommodation and associated travel services	Performance of a contract with the party leader; legitimate interests in providing arrangements to all party members; and legal obligations where applicable.
Contact guests about payments, documents, changes, disruption, arrival, access, safety, complaints and other service matters	Contract; legitimate interests in effective service and safety; legal obligation; and vital interests in an emergency.
Process payments, refunds, accounts, tax and audit records	Contract; legal obligation; and legitimate interests in financial administration, fraud prevention and audit.
Handle accessibility or other information that reveals special category data	An ordinary lawful basis above plus, normally, explicit consent for the special category element; vital interests or legal claims where the relevant statutory condition applies. Such category data is deleted unless stated as otherwise.
Improve services, invite and assess feedback, and produce aggregated statistics	Legitimate interests in quality, training and service improvement. Marketing content remains subject to the marketing rules below.
Record calls, maintain correspondence and protect staff, customers, systems and property	Legitimate interests in accurate records, training, security, preventing and detecting misuse or fraud, and resolving issues; and legal obligation where applicable.
Establish, exercise or defend complaints, debts, insurance matters and legal claims	Legitimate interests, legal obligation and the statutory conditions for legal proceedings, obtaining legal advice and establishing, exercising or defending legal rights or claims.
Send direct marketing and measure campaigns	Consent where required. Where legally permitted, we may rely on legitimate interests or an applicable existing-customer or 'soft opt-in' rule, always with a clear opportunity to object or unsubscribe.
Operate, secure, analyse and personalise our website and digital services	Strictly necessary processing for contract, security and legitimate interests; consent for non-essential analytics, advertising or storage/access technologies where required.

Data minimisation and purpose limitation

We collect personal data that is adequate, relevant and limited to what is necessary for each stated purpose. We do not collect information merely because it may be useful later. We periodically review fields, access permissions, copies and retention periods; restrict special category and identity information; redact or remove unnecessary material; and anonymise data where the purpose can be achieved without identifying anyone. We will not use personal data for a new and incompatible purpose without identifying a lawful basis and giving any further notice required.

6. Booking and service communications

We may contact the party leader and, where appropriate, other party members by telephone, voicemail, email, SMS, WhatsApp, live chat, social media messaging, post or another channel they use or agree to use. We use these channels to administer enquiries and bookings, take requested action, send documents, collect necessary information, respond to questions, deal with disruption or emergencies and provide important service or policy notices.

These operational contacts are not direct marketing merely because they are sent electronically. Withdrawing marketing consent or unsubscribing does not prevent necessary booking, safety, legal or service messages. You may tell us your preferred channel, but urgent circumstances, delivery failure, security or the nature of the matter may require another reasonable method.

WhatsApp and external messaging platforms

If you initiate contact through WhatsApp or another external messaging platform, or agree to use it, the platform provider may process message content, telephone numbers, device and usage metadata under its own terms and privacy information, including outside Jersey. We retain relevant business communications in our systems where necessary. Please avoid sending full payment-card details, passport copies or detailed medical information through a general messaging service unless we have specifically asked you to use a secure method.

7. Direct marketing

Marketing may be sent by email, SMS, WhatsApp or similar electronic messaging, telephone, post, online advertising or social media. We distinguish marketing from communications needed to provide or administer a booking.

For unsolicited electronic marketing to an individual, our default is a clear, specific opt-in for the organisation and channel. Where an applicable law permits an existing-customer or soft opt-in approach, it will only be used for our own similar products or services after a clear opt-out was offered when the contact details were obtained and in every later message. We do not use pre-ticked consent boxes.

Every marketing message will provide an appropriate way to object or unsubscribe. You can also change your preferences by contacting marketing@macoles.com. We keep a limited suppression record after an objection so that we do not contact you again by mistake. We do not sell personal data or disclose it to another organisation for that organisation's independent marketing without specific permission.

Your absolute right to object to direct marketing

You may object at any time to our use of your personal data for direct marketing, including related profiling. Once we receive the objection, we will stop that processing. This right is separate from our continued use of information needed to administer an active booking or meet legal obligations.

8. Email delivery and engagement tracking

Our email service records dispatch, delivery, delay, bounce, spam-complaint and unsubscribe events. We use these records to deliver messages, maintain accurate contact data, protect our sending systems, evidence communications where proportionate and troubleshoot failures.

Where enabled, a tracking pixel or coded link may indicate that an email was opened or a link selected and may provide the time, IP address, approximate location and device or browser information. Open data is not conclusive: security systems, image blocking and privacy services can create or prevent an event. We will not treat the absence of an open event as proof that a message was not received or read.

For marketing emails, we use engagement tracking only where we have an appropriate lawful basis and obtain consent to storage or access technology where required. Tracking must not be hidden behind acceptance of this Statement. For essential booking and administrative messages, we use delivery and security events as necessary; optional open or click analytics should be disabled unless separately justified, transparent and permitted.

9. Cookies, pixels, analytics and similar technologies

Our website uses essential technologies needed for functions such as security, session continuity, consent choices, booking and payments. It may also use non-essential analytics, advertising, conversion, personalisation, chat or embedded-content technologies, including services supplied by Google, Meta/Facebook, Conversiobot, 3CX and mapping or media providers.

We ask for a valid choice before setting or accessing non-essential technologies where consent is required. Rejecting non-essential technologies must be as straightforward as accepting them. You can change your choice through the website's cookie controls. Blocking essential technologies may prevent parts of the booking service from working.

A current cookie inventory should identify each technology, provider, purpose and duration. Because this information changes more often than the main Statement, we may publish it as a separate Cookie Policy or within a consent-management panel. The current Cookie Policy or panel forms part of the privacy information we provide and should be read with this Statement.

10. Special category data and children

Accessibility, dietary, religious or other special requests can reveal sensitive information. Please provide only what is necessary to arrange the service. We ask you not to disclose specific medical information, as we do not require diagnosis or details and are not qualified to interpret it, rendering it useless to our function. Explicit consent before recording or sharing the special category element, unless another specific legal condition applies. We limit access and disclose only information to suppliers that is needed to fulfil a request, safety or legal claim.

Bookings often include children. We use children's names, ages, travel and safety information only as necessary for the booking, supplier rules and legal requirements. We do not intentionally direct marketing to children or ask a child to consent to marketing. The party leader or a person with appropriate authority should provide the child's information.

11. Who we share personal data with

We disclose only what is reasonably necessary to the following categories of recipient:

- Accommodation owners, managers, providers, key holders and on-island support services.
- Ferry companies, airlines, transport operators, ground handlers and other travel suppliers where included in or connected with the requested arrangements.
- Payment processors, acquiring banks, banks, refund and fraud-prevention providers.
- Providers of booking, customer-management, accounting, document, cloud hosting, email, website, telephony, call-recording, chat, analytics, advertising, security, backup and IT-support services.
- Insurers, insurance brokers, accountants, auditors and other professional advisers.
- Government departments, immigration or customs authorities, regulators, tax authorities, police and other public authorities where required or permitted by law.
- A prospective purchaser, investor or successor as part of a genuine business reorganisation or sale, subject to appropriate confidentiality and necessity controls.

Some service providers act as processors on our instructions and may use authorised sub-processors. These are sometimes informally called 'fourth parties'. That is not a separate legal category: we require appropriate contractual, confidentiality, security, assistance and deletion obligations and remain responsible for selecting and overseeing processors as required by law.

Disputes, claims and litigation

Where a complaint, chargeback, debt, insurance matter, threatened claim, alternative dispute resolution process or litigation arises, we may provide relevant personal data to the other parties and their authorised representatives; accommodation or travel suppliers; insurers and claims handlers; lawyers and other advisers; experts, witnesses, mediators, arbitrators, courts, tribunals, enforcement officers, debt-recovery providers, e-disclosure or IT providers; regulators and public authorities. Disclosure will be limited to information reasonably necessary to obtain advice, investigate, preserve evidence, comply with a duty or order, recover a debt, or establish, exercise or defend legal rights. It does not depend on blanket consent.

12. International transfers

Travel arrangements and our technology suppliers can require personal data to be accessed from or transferred to the UK, European Economic Area, United States, the destination of travel or another country outside Jersey. Protection may differ from Jersey law.

We use a transfer mechanism permitted by the DPJL 2018, such as an adequate jurisdiction, approved or appropriate contractual and organisational safeguards, or a limited statutory exception - for example, a transfer necessary to perform a contract requested by you or to establish, exercise or defend legal rights. We assess and document restricted transfers as required. You may ask us for further information about the relevant destination and safeguards, subject to lawful confidentiality restrictions.

13. How long we keep personal data

We do not retain identifiable data longer than necessary. The following are normal maximum periods or review points, not automatic entitlements to keep every field for the whole period. A shorter period

is used where the purpose has ended and a longer period only where law, audit, fraud, safeguarding, complaint, debt or legal hold requires it.

Record type	Normal retention or review point
Unsuccessful enquiry or quotation	Normally 24 months after the last substantive contact.
Booking administration and ordinary customer-service correspondence	Normally up to 6 years after departure or cancellation, with earlier deletion or anonymisation of unnecessary identity, travel and special-request data.
Accounting, invoice and transaction records	At least 10 years from creation where they are accounting records required by the Companies (Jersey) Law 1991; personal detail is limited to what the record requires.
Call recordings	Normally 90 days, unless selected for training, complaint, safeguarding, fraud, debt or legal evidence, in which case the relevant extract or record follows the related case period.
Website, security and technical logs	Normally up to 12 months, unless required for an active security incident or legal matter.
Email open and click analytics	Normally up to 24 months, then deleted or aggregated, unless attached to a complaint, consent record or legal matter.
Marketing contact and engagement history	While permission or another lawful basis remains current; reviewed after 24 months of inactivity and normally removed from active marketing after 5 years without engagement. A minimal suppression record may be retained to respect an objection.
Disputes, complaints, debts, insurance and litigation	Until final resolution and for the applicable legal, regulatory or prescription period, or while a documented legal hold applies.

14. Your rights

Depending on the processing and lawful basis, you may have the right to:

- be informed about how your personal data is used;
- obtain access to your personal data and a copy of it;
- correct inaccurate or incomplete data;
- request erasure in circumstances where the law requires it;
- restrict processing in specified circumstances;
- receive data you provided in a structured, commonly used, machine-readable format and ask for it to be transmitted where the portability conditions apply;
- object to processing based on legitimate interests and object absolutely to direct marketing;
- withdraw consent at any time where consent is the basis, without affecting earlier lawful processing; and
- not be subject to a solely automated decision that produces legal or similarly significant effects, subject to statutory exceptions and safeguards.

Rights are not unlimited. For example, erasure does not apply where data remains necessary for a legal obligation, accounting record, unresolved booking, debt, complaint or legal claim. We will explain any refusal or restriction.

You can make a request verbally or in writing using any contact method in section 1. Please describe the right and information concerned. We may request proportionate proof of identity or authority and will use a secure response method. Requests are normally free, although the law permits limited exceptions.

15. New and future technologies

We may introduce a new communication channel or technology that performs a substantially similar function to email, SMS, telephone, messaging, booking, payment, fraud prevention, analytics or customer support. This Statement is intended to remain technology-neutral, but it is not advance permission for every future use.

Before using personal data through a technology that creates a materially different purpose, category of data, recipient, international transfer, monitoring activity, automated decision or privacy risk, we will assess necessity and proportionality, apply data protection by design and default, complete a data protection impact assessment where required, update our privacy information and obtain consent where the law requires it. We will not use personal data for facial recognition, biometric identification, intrusive behavioural monitoring or solely automated significant decisions merely because a broad 'future technologies' phrase appears here.

16. Automated decision-making and profiling

We do not currently make decisions about a booking that are based solely on automated processing and produce legal or similarly significant effects. We may use limited segmentation or personalisation for marketing and service improvement, subject to transparency, lawful basis and the right to object. If significant automated decision-making is introduced, we will explain the logic, significance and likely consequences and provide applicable safeguards, including human review.

17. Security and data breaches

We use proportionate technical and organisational measures designed to protect personal data against unauthorised or unlawful processing and accidental loss, destruction or damage. Measures include access control, staff confidentiality and training, supplier due diligence and contracts, backups, system maintenance, secure payment handling, incident management and appropriate encryption or pseudonymisation.

No system is completely secure. We investigate suspected breaches, keep required records and, where notification is required, notify the Jersey Office of the Information Commissioner without undue delay and, where feasible, within 72 hours. We notify affected people where the law requires it.

18. Related policies, terms and third-party services

This Statement should be read with our Essential Reading Terms & Conditions, website or acceptable-use terms, cookie information and any short privacy information shown when data is collected. These documents have different functions:

- The Essential Reading Terms & Conditions govern the booking contract and responsibilities of the party leader and party members.

- This Statement explains how personal data is processed. Acceptance of the booking terms is not consent to marketing, and contractual wording does not remove statutory data protection rights.
- The Cookie Policy or consent panel gives the current technical inventory and controls for cookies, pixels and similar technologies.
- A supplier or platform acting as an independent controller - for example a payment service, airline, ferry operator, accommodation provider or messaging platform - may also provide its own privacy notice. Its notice does not replace ours for processing for which we are responsible.

Essential Reading Terms & Conditions: www.macoles.com/PDFs/Macoles_Terms_conditions.pdf

If contractual wording and this Statement appear inconsistent, we will interpret them so far as possible consistently with applicable data protection law; the law prevails where it cannot be reconciled.

19. Changes to this Statement

We review this Statement periodically and when our services, suppliers, technologies or legal obligations change. The current version and issue date will be published on our website. If a change is material, we will take proportionate steps to bring it to the attention of affected people before the new processing begins, and obtain fresh consent where required. A service notice about a privacy change may still be sent to a person who has opted out of marketing.

20. Complaints and contact

Please contact us first if you have a question or concern. We will try to resolve it promptly. You may also complain directly to the Jersey Office of the Information Commissioner (JOIC):

Jersey Office of the Information Commissioner, 2nd Floor, 5 Castle Street, St Helier, Jersey, JE2 3BT | +44 (0)1534 716530 | enquiries@jerseyoic.org

www.jerseyoic.org

Where UK data protection law applies to the relevant processing, you may also complain to the UK Information Commissioner's Office.

www.ico.org.uk/make-a-complaint

Legal framework

This Statement has been drafted principally against Article 12 and the data protection principles, lawful bases, individual rights, processor, security and international-transfer provisions of the Data Protection (Jersey) Law 2018, together with current JOIC privacy-notice guidance. UK ICO guidance has been used as best-practice support and where UK law may apply.