

SOMERSET COURT COTTAGES LTD

DATA PRIVACY POLICY

Your Data and Information is Safe in our Hands

When we use the term “Our Website” we are referring to this website. When we use the terms “Our Company”, “Our Business”, “Us”, “We”, or “Our” we are referring to our Company, Somerset Court Cottages Ltd.

When we refer to “information” we are referring to data, either recognisable or anonymous.

The Data Protection Act 1998 and The General Data Protection Regulation.

We process your data in accordance with the Data Protection Act and the GDPR under UK Law. The purpose of this privacy policy is to inform anyone who may potentially send us their personal data and to identify the data that we are willing to receive.

It covers:

- a) Why we request data and what data we are willing to accept.
- b) How long we retain this data (legal requirement or business requirement)
- c) If data is disclosed to a 3rd party.
- d) How you can find out what data we hold about you, and your right to request erasure or restricted processing, where data is not held and processed as a requirement by UK Law or a UK regulatory requirement.

Strictly no Special or Sensitive information will be requested or should be submitted, emailed or transmitted to us via email or any other contact method.

To process an enquiry you may have, we only accept the following personal data. Full Name, Telephone Number, Email address, along with your enquiry, so that we can reply to the enquiry.

To process a booking or order, we will only accept the following personal data. Full Name, Telephone Number, Email address, along with your booking information so that we can process your booking.

To process an online deposit, part payment or full payment online, we use a PCI-DSS Level One compliant and approved booking system and payment gateway to accept your card payment, as required by Debit and Credit card companies.

We want you to feel secure when visiting our website, submitting form data or sending us emails, and we are committed to respecting your privacy. Below we give an overview of how we do that.

Your Data and Information Safe in our Hands

1: The personal data we collect from our website or email:

- We collect personal data Indirectly and Directly.
- We collect Recognisable Personal data and Anonymous data.

Website Access, Recognisable Data: When you access our website our web hosting servers store certain data indirectly within daily access logs. This recognisable data contains your external internet I.P address only. This data is used solely for fraud detection, to detect malicious attacks or unauthorised access, and for maintaining the general security and traffic management of our systems. Based upon this information certain IP addresses or IP address ranges that overuse bandwidth or cause a security concern will at our discretion be banned or blocked from connecting to our website. These IP addresses will be stored and processed for a period of 5 years, but reviewed annually to see if any IP addresses no longer pose an issue to our data, systems and networks. All other daily access log data will be erased within 30 days from that IP's daily connection.

Anonymous Data & Cookies: Because we comply with the EU/UK Cookie Law, we ensure that we have made you aware of the cookies that we use and our privacy policy related to them. We do this by displaying this information to you as a popup, and we then save a cookie to your device. This cookie is an anonymous cookie, which cannot be used by us or others to recognise you or your device. The cookie is named EUCookiedirective and the data is "IMPLIEDCONSENT", this cookie is expired on your device every 30 days, and we will repeat the action above when that cookie has expired.

Contact Recognisable Data: We also collect data when you give it to us. For example, you may email us by using a link from our website or by using a website form to pass the information that we have requested from you, for us to reply to your enquiry. When we collect this type of information, we will notify you as to why we are asking for it and how this information will be processed, for how long it will be retained, and with whom it will be shared.

Recognisable Data & Cookies from Social & Media networks: This covers when you visit our social media pages, or pages which are supplied by online media networks that represent our business (such as Twitter, Facebook, Google, Bing, Tripadvisor, Instagram, LinkedIn, Youtube or any other media). The privacy policy, data policy and cookie policy of that online media network applies to any data they will process. You have already accepted this via your account with them. Please see the service providers own Privacy and Cookie policy for further information.

Your Data and Information is Safe in our Hands

2: Data Processing & Retention – We retain the following data because a legal requirement or business requirement

- a) Our Business – Enquiries not resulting in a purchase, 30 days
- b) Our Business – Booking or Order Cancellations, 5 years
- c) Our Business – Refunds or Credit Notes, 5 years
- d) Our Business – Threat or Potential of Legal Action, 15 years
- e) Our Business – Other data not covered by UK regulations/law, 3 years
- f) Companies Act/HMRC – sales/purchasing/cash/payments data for 6+1 years.
- g) Taxes Management Act - Payroll for 6+1
- h) The Reporting of Injuries 1995 - Accident Incidents 3 years past date
- i) Discrimination Acts/Race Relations – job application unsuccessful, 6 months
- j) SSP Regulation - Sickness, 3 years after end of tax year
- k) Limitations Act 1960 - Leases, fifteen years after expiry
- l) DPA - Pension Scheme, 6 years after death
- m) DPA - Insurance records, 3 years post lapse
- n) Employers' Liability regulation – insurance certificates 40 years
- o) DPA - Claims Correspondence, 3 years after settlement
- p) Companies Act - Health and Safety permanent

This data processing and retention policy is provided to demonstrate the retention period of data, when that data is sent to us via our online websites, 3rd party websites, social media or via direct or indirect email communications. This policy is subject to change when either required by UK law or to better align our data processing, archiving and retention policy in accordance with UK regulation, legal requirements or lawful business requirements.

2: How do we use information?

We may request or accept information from you in order to process an enquiry you have regarding the service that we provide.

We also take and process data regarding sales and purchases (you make) and retain and process that data within the confines of UK regulations and laws, including the GDPR.

We may also use data for other purposes, which we would inform and describe to you at the point at which we collect that information.

When we request information within a form, for example an Enquiry or Booking form or a Contact form, we will display a link to this document and ask you if you are happy with this Privacy Policy before you submit your information.

Your Data and Information is Safe in our Hands

3: Do we disclose or Share your information with other organisations.

Your data can be collected by our own enquiry or booking facilities, or by our payment gateway provider. In this case our partner, who is authorised by us to take this data, will provide you with a privacy policy and will outline why data is be taken and how it will be processed and for how long it will be retained.

We do not share any of your data with any other organisations unless the law permits us to do so.

We do not sell individual information.

We will share data only with our authorised Data Processors, who must act at all times on our instructions as the Data Controller within the confines of the Data Protection Act 1998 and the General Data Protection Regulation.

Before you submit any information, we will notify you as to why we are asking for specific information and it is up to you whether you provide it.

4: Access to Data/Information we hold about you.

You are entitled to know whether we hold information about you and if we do, to have access to that information and require it to be corrected if it is inaccurate.

You can also request that any data we have be erased or have a restricted processing policy placed upon it, unless there is a legal requirement or business reasons why it cannot be, in which case we will offer a full explanation for any rejection for that request.

You can do this by contacting us via email through our website and addressing the subject and/or body to “The Data Protection Officer”. Your data is kept secure as required by the data protection act (GDPR).

Your Data and Information is Safe in our Hands

5: Security

We take appropriate steps to maintain the security of your Online data when it is stored in the Cloud.

- a) Hosting for this website is located within a secure Data Centre, monitored by CCTV, and accessible only by approved personnel with specific security privileges based on the data centre requirements.
- b) The information contained within our hosting space and associated hosting services are secured with appropriate firewall policies and security permissions as well as authentication levels of access.
- c) Emails using the e-mail facility supplied by our web hosting company can also be received or sent using secure connections.
- d) Where we request card payments, an appropriate payment taking service and/or Gateway provider will take card payments on our behalf. They will have a compliant pci-dss compliancy level as required by the credit and debit card companies.

We take appropriate steps to maintain the security of your Offline data stored within our own local storage solutions.

- a) Where we request card payments via Chip and Pin or Payment Card Not Present payments, we are pci-dss certified and undertake regular quarterly scanning as required by the Debit and Card companies PCI-DSS compliancy requirements.

The open nature of the internet means that your data may flow over networks without security measures and may be accessed and used by people other than those for whom the data is intended.

Our intention is that this should not happen and we take measures to ensure that it does not, though we advise that all individuals who submit personal information to us, do not use Open Wi-fi or free secured wi-fi networks to communicate their data to us, without using secure email SSL or TLS connections or secure website communications to add an additional security measure to the data that they are sending.

6: For our Online Visitors Piece of Mind

We do not use 3rd party Analytics services which often conflict with an explicit “Do Not Track” setting which has been configured in a modern browser. If you wish to block all tracking, the new Mozilla browser, Options / Privacy & Security / Tracking Protection seems to stop all analytics being executed.