

# Privacy Policy

## 'Your Data & Us'

Policy date:	05 March 2024	
Date of next review:	by 05 March 2025	
Approved by:	DB	
Intended for:	Guests & members of public	
Location (tick as appropriate):	Websites	✓
	Reception	✓
	Management Folders	✓
	Company Computers	✓

**Registered Office:**  
Sandringham Hotel  
Esplanade  
Sandown, Isle of Wight  
PO36 8AH

**Details:**  
+44 (0)1983 405555  
DPO@iwhotels.co.uk  
Company no. 01812172 / 01303729  
ICO reg no. ZA 44 99 55 / ZA 44 99 52

## **Definitions:**

“We”, “Company”, “Business”, “Our”, “Us”, “Data Controller” means Isle of Wight Hotels Ltd and Sandringham Hotels (Isle of Wight) Limited or subsidiaries and assets belonging to them.

“Property”, “Premises”, “Accommodation” means Sandringham Hotel, Calverts Hotel, Clifton Seafront Apartments, Sandown Hotel, Bay View, Regent Court, Old Police Station, Royal York Hotel, Grand Hotel and their associated bars, venues, facilities or other undesignated function rooms.

“Data Protection Officer” means Mr. D. Banks and Miss. K. G. Moorman, executives of the company.

“You”, “Your”, “Client”, “Guest”, “Occupier”, “Data Subject” means the lead booker, guests occupying accommodation or in general any other persons / organisations.

## **Introduction:**

In order for us to undertake, streamline and secure our day-to-day business operations, we are required to collect information from you, the data subject.

The company is a responsible data controller, and we take your privacy and the protection of your data very seriously. We are compliant with The Data Protection Act 2018 and General Data Protection Regulation (GDPR) and are registered with the Information Commissioner's Office (ICO).

This privacy policy applies to you when you reserve and are occupying accommodation with us, or when visiting our websites or premises for any reason.

This policy does not apply to employees of the company – consult the employee handbook.

If you do not agree with our privacy policy, then you should cease use of our websites and services and contact our reservations team by telephone to make any further enquiries.

The company will not be liable for any refund or compensation in such circumstances.

This policy is subject to change or redaction at any time, for any reason.

## **Your Information:**

Any personal information you provide us with online (booking pages, contact form etc) or by telephone will be stored in our online booking system and channel manager, Freetobook, as per our data retention policy. This includes, but may not be limited to:

- Full name
- E-mail address
- Telephone number(s)
- Home / billing address
- A token linked to the payment card you used (via Stripe)
- Dietary requirements
- Disabilities and/or other health conditions
- Special requests – birthdays, anniversaries etc

We reserve the right to collect and store a physical paper copy of your information: booking confirmation, phone number, address and copy of your photo ID. This will be stored and destroyed in-line with our retention policy.

If you make your reservation through a third party agency or booking website (i.e. Booking.com) they will also store your data you provide them – please refer to their privacy policy or data processing statement; we have no control these sites/agencies.

We will retain all communications and details sent to us by post or by e-mail, including information submitted through our contact forms, until it is deemed necessary.

We reserve the right to record and monitor telephone calls. If recording is being used, you will be informed of this at the start of the call.

If we book your ferry travel for you, we will need to share a limited amount of your information to the ferry operators.

We will share any dietary requirements with our catering team. We will share any disabilities with reception, night porter and housekeeping teams.

We will not write down or store your full payment card details. We will not collect information from you that is not required for us to undertake our business operations.

CCTV video recording is in use across the public and exterior locations on our premises, for your safety and our security; audio recording is used in transaction locations (reception and bar), to prevent fraud and to assist with any guest complaints which may arise.

CCTV is not provided in guest accommodation, nor in sensitive locations. It is, however, in use in any swimming / bathing / spa facilities for personal safety only, as per our risk assessment and PSOP.

CCTV recordings are kept for no longer than 31 days, and then overwritten. CCTV servers are kept in secure rooms with locked doors or in a locked cabinet.

Your personal data will never leave our audited systems or premises.

### **Reservations:**

All reservation data is stored by US Booking Services Limited (Freetobook), our chosen provider.

Third party booking sites also store guest data on their servers, which we can login to and access.

Our central reservations office is located at our registered office address.

We will only speak to you, the lead guest/booker, on the telephone – no one else.

We will only respond to e-mails regarding your reservation to the e-mail address we hold for you.

We will only post letters / correspondence to the address we hold for you.

To facilitate this, we will always ask you to confirm at least two pieces of personal information we already know about you. If the caller is unable to verify this, we will not disclose any information about you or your reservation; nor allow any amendments or additions.

## **Payments:**

We are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

Online payments are processed with the help of Stripe; a token linked to your payment card is stored in our selected booking system provider (Freetobook) until your departure date to facilitate amendments, fees, additional incurred costs or refunds which may need to be made.

The Strong Customer Authentication Regulation requires the use of 3DS for online card payments – you may be asked to verify payments to us using your card provider’s mobile app or by SMS text message.

Reservations made through a third party agency or website (i.e. Booking.com) collect payment directly from you. They will have their own payment processing statements and therefore this section of the policy will not apply to you.

Payments made to us in-person will be by completed on Dojo card terminals by chip & PIN, contactless or NFC. We do not accept signature / swipe card payments as these carry a high risk of fraud. Our card / PDQ machines do not store cardholder information.

## **Retention:**

Data stored within Freetobook is retained for seven years, then deleted forever by Freetobook and removed from their servers.

A token linked to your payment card is stored until your booked departure date.

Physical paper copies of information are retained for seven years in a secure in-house facility; then collected by a local confidential waste destruction company to be destroyed.

Destroyed physical data / paperwork is certificated.

We do not store any digital information on our own systems or servers.

We are required to store all records for seven years, in-line with His Majesty’s Revenue & Customs (HMRC) auditing guidelines.

If you misplace your payment card or photo ID on our premises, we will hold it in our safe at reception until your planned / booked departure. If it is not collected prior to your departure then it will be destroyed (shredded) on-site at the earliest opportunity – we will not be able to post these back to you.

Data collected for network diagnostics are retained for six months, then deleted automatically.

### **Third Parties:**

We will not share or disclose any information about you to unrelated / unnecessary third parties.

If we book your ferry travel for you, we will share your name, phone number and vehicle registration with Red Funnel (SOUTHAMPTON ISLE OF WIGHT AND SOUTH OF ENGLAND ROYAL MAIL STEAM PACKET COMPANY LIMITED) or Wightlink Limited. In this case, the ferry operators are the data controllers.

We are legally required to share certain information we hold/know about you to authorities such as police forces, national crime agency, action fraud etc upon request from them. This could include:

- Your full name
- Your contact details, including address
- CCTV video & audio footage whilst on or around our premises (if applicable)
- Dates of your reservation(s)
- Evidence of any criminal activity
- Receipts and invoices showing purchases

In the event an accident or injury occurs on our premises requiring us to inform the Health and Safety Executive (HSE) under RIDDOR we will share with them:

- Your full name
- Your contact details, including address
- Date of incident / accident
- Nature of incident / accident
- Date of birth
- Your statement of events
- Declared health conditions & disabilities

We will not make you aware of submissions we have legally had to make to Government / Local Authorities.

Although we do not and will not, if we do decide that we wish to share your information with any other third party, we will always seek your permission in writing first.

### **Websites & Cookies:**

Our websites and booking pages (freetobook.com) use cookies to better improve your online experience.

If you wish to opt out of cookies, please make your reservation by telephone 01983 405555.

We have no control over cookies Freetobook utilise.

To further keep your information safe, our websites and booking pages use SSL encryption, as indicated by the secure symbol on the address bar of your chosen browser.

Our websites use Google Analytics, which uses cookies to analyse how users (you) interact with the site. The information generated by the cookie about your use of the website, including your IP address, will be stored by Google (Alphabet Inc).

Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and the company; providing other services relating to website activity and internet usage.

## **Networks, Computers & VOIP:**

Only permitted and trained employees are permitted to use company computer and devices.

Our computers have anti-virus and anti-spyware software installed. Computer updates / software patches are automatically installed as soon as they're released, or at the earliest opportunity.

Passwords are changed quarterly to prevent unauthorised access to personal data and systems.

Our wired and wireless (Wi-Fi) networks store basic data used for internal diagnostic and improvement purposes only. Data collected includes:

- Local IP address
- Device MAC address
- Device hostname (e.g. Jon's iPhone)
- Connection time
- Access point connection & movement/handoff information

Separate terms and conditions are in place for this facility.

Our multi-site VOIP telephone system is provided by British Telecommunications Plc. Call records (inbound and outbound) and voicemail messages are stored on BT's online portal / servers and on the local extensions for a maximum of 30 days. We do not operate a directory system nor a CMS.

Our chosen ISPs are WightFibre Limited and British Telecommunications Plc. DNS lookups are not stored by us but may be by the ISP – this is out of our control.

## **Team Members & Training:**

Training of our employees is undertaken in-house on a regular basis, or at least a refresher is undertaken every 12 months.

We have 100% trust in our faithful and longstanding workforce. They all understand the seriousness surrounding the protection of personal data; themselves being data subjects throughout daily life.

Departments with access to guest data; therefore included in regular training sessions are:

- Receptionists & Night Porters
- Reservation Clerks
- Management / Team Leaders

Departments where training is not provided; instead, basic information is included in employee handbook due to very little or no interaction with data subjects' information:

- Waitstaff, Bartenders & Catering
- Maintenance & Estates
- Housekeeping
- Non-Executive Directors

Any new legislation, updates or tips are communicated to the reception and reservation teams immediately facilitated by the senior management team and/or the data protection officers. Any additional members of the team are fully trained prior to handling data.

Auditing is in place so that employees can be held accountable for malicious acts including, but not limited to, unlawful distribution and/or sharing of data. CCTV recordings are only accessible by 2 x members of the senior management team.

### **(Unsuspecting) Members Of The Public:**

Those utilising the company's bars or other non-designated facilities/rooms within our premises will become data subjects by means of CCTV recordings and if they provide us with any other contact information.

Receipts / invoices will always be provided but can always be requested by the data subject at a later date.

Those walking or travelling past, but close and adjacent to, the exterior of the company's premises will ultimately become data subjects by means of being captured on CCTV recordings.

CCTV recording of the adjacent pavement areas are absolutely required by the company for:

- General security.
- Damages caused to doors, windows, structure, or graffiti.
- Auditing of deliveries.

Members of the public therefore also have a right to a copy of their video recording / data.

### **In The Event Of A Data Breach:**

In the first instance, we will conduct a swift internal investigation to determine how the breach has occurred, and who has been affected.

We will contact the Information Commissioners Office (ICO) to inform them of the breach and take any further action they require / recommend us to do. We will contact Hampshire & Isle of Wight Constabulary to report the crime and any evidence.

We will contact all data subjects affected by the breach.

We have a cyber indemnity policy in place to cover any damages, and we will seek independent legal advice from our chosen firm: Roach Pittis Solicitors Limited.

Breaches affecting you where we will not be liable:

- If Freetobook has a data breach, they will initially contact us. We will then inform you by forwarding-on correspondence from Freetobook.
- If a third party booking agency or website (i.e. Booking.com) has a data breach, they will contact you directly.
- If Red Funnel or Wightlink have a breach, they will contact us, and we will then inform you.

### **Your Rights:**

You have a right to a copy of the data we hold about you, including but not limited to:

- Contact details
- CCTV video and audio recordings
- Accident records
- Registration forms / photo ID collected from check-in
- Receipts and invoices
- Restaurant and bar orders
- Telephone notes made by reservations team
- E-mail and postal correspondence
- Telephone recordings

To make this request, please do so by e-mailing **DPO@iwhotels.co.uk** or writing to the 'Data Protection Officer' at our registered office: Sandringham Hotel, Esplanade, Sandown, Isle of Wight, PO36 8AH, United Kingdom.

We reserve the right to charge a reasonable fee for administration on successful requests. We will endeavour to respond within 30 days of receiving your request.

If a request cannot be fully fulfilled, or only partly fulfilled, the data protection officer will contact you by telephone, by post, or by e-mail at the earliest opportunity.

Please note: our business is not subject to 'The Freedom of Information Act 2000'.

Please ensure you also read terms and conditions – <https://isleofwight.info/Terms-Conditions.pdf>