

Privacy & Data Protection Policy

Policy date:	17 February 2026	
Date of next review:	by 17 February 2027	
Authored / approved by:	DB, KGM, HJB	
Intended for:	Guests & members of public	
Location (tick as appropriate):	Websites	✓
	Reception	✓
	Management Folders	✓
	Company Computers	✓

1. Definitions

Our structure is formed of two sister companies. This document covers both legal entities.

“We”, “Company”, “Our”, “Us”, “Data Controller”, “Controller” means:

Isle of Wight Hotels Ltd, a company registered in England and Wales, registration number: 01812172 with its registered office at or being Sandringham Hotel, Esplanade, Sandown, Isle of Wight, PO36 8AH. ICO registration number: ZA 44 99 55.

Sandringham Hotels (Isle of Wight) Limited, a company registered in England and Wales, registration number: 01303729 with its registered office at or being Sandringham Hotel, Esplanade, Sandown, Isle of Wight, PO36 8AH. ICO registration number: ZA 44 99 52.

and any subsidiaries companies.

“Business”, “Property”, “Premises”, “Accommodation” means:

Sandringham Hotel, Esplanade, Sandown, Isle of Wight, PO36 8AH
 Sandringham Hotel trading as Regent Court, Sandown, Isle of Wight, PO36 8AH
 Sandringham Hotel trading as Bay View, Sandown, Isle of Wight, PO36 8AH
 Calverts Hotel, 27-29 Quay Street, Newport, Isle of Wight, PO30 5BA
 Sandown Hotel, 1-3 Culver Parade, Sandown, Isle of Wight, PO36 8AS
 Clifton Seafront Apartments, C/o Sandringham Hotel, Sandown, Isle of Wight, PO36 8AH
 Royal York Hotel, 67 George Street, Ryde, Isle of Wight, PO33 2ES
 Grand Hotel, Culver Parade, Sandown, Isle of Wight, PO36 8QA

and other assets including bars, clubs, venues, facilities or other unspecific function rooms.

“You”, “Your”, “Client”, “Guest”, “Occupier”, “Consumer”, “Subject” means:

The person(s) entering into the contract, the lead booker and/or payer, guest(s) occupying accommodation or any other persons / organisations listed on a reservation, receipt, invoice or reservation clerk’s booking notes.

“Data Protection Officer” means:

Mr. D. Banks care-of the company’s registered office address.

“Site”, “Website”, “Page” means:

www.sandringhamhotel.co.uk; www.calvertshotel.co.uk; www.sandownhotel.co.uk;
www.cliftonseafontapartments.co.uk; and/or: isleofwight.info And all pages and sub-links.

“ICO” means:

[The] Information Commissioner’s Office

“Booking office”, “Reservations office” means:

The company’s registered office address, or another above address in the event of an unforeseen circumstance thereby activating our business continuity policy and plans.

2. Website terms

By [continuing to] browse and use this website you agree to comply with and be bound by the following terms and conditions of use and privacy policy. Our relationship is with you in relation to this website. If you disagree with any part of these terms and conditions, please cease to use our website and contact us by telephone 01983 405555.

Scope:

The content of the pages of this website is for your general information and use only. It is subject to change at any time and without notice.

Our website(s) and booking pages (Freetobook / booking-directly.com) use cookies and similar trackers to monitor browsing preferences and 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 or influence over cookies Freetobook [may] utilise.

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.

Our rights:

Neither we nor any third party provide any warranty or guarantee as to the accuracy, timeliness, performance, completeness or suitability of the information, content and materials found or offered on this website for any particular purpose. You acknowledge that such information and materials may contain inaccuracies or errors; we expressly exclude liability for any such inaccuracies or errors to the fullest extent permitted by law.

Your use of any information, content or material on this website is entirely at your own risk, for which we shall not be liable. It shall be your own responsibility to ensure that any product or service is error or virus-free.

Unauthorised use of this website may give rise to a claim for damages and/or be a criminal offence.

From time to time, this website may also include links to other websites or content (photos) from other sites. These links and content are provided for your convenience to provide further information. They do not signify that we endorse the website(s) or their services. We have no responsibility for the content of said linked website(s).

Your use of this website and any dispute arising out of such use of the website is subject to the laws of England, Wales, Scotland and Northern Ireland only.

3. Introduction

Scope:

In order for us to undertake, operate, streamline and secure our day-to-day business operations we are required to collect information from you, the data subject. This policy applies to you when you reserve and are occupying accommodation, and/or when visiting our websites or premises for any other reason.

The company respects your privacy and is committed to ensuring your data and personal information is kept and processed in a secure way. We are registered with the ICO; will only process your data in accordance with this policy and the Data Protection Act 2018. This policy includes the information we collect about you when you provide it to us or use our website(s), products or services, as well as how we process your data.

We reserve the right to amend this policy from time to time by way of updating this document (page). You should check this page each time to ensure that you are happy with any changes. This document and policy are valid and effective as per the policy date on the cover page.

All data about you will be stored in-line with our retention policy – section 8 – unless otherwise stated.

The data protection officer can be contacted by emailing DPO@iwhotels.co.uk or in writing to the 'Data Protection Officer' at the company's registered office address.

What is personal data:

Any information relating to a person who can be directly or indirectly identified based on that information, as outlined by England and Wales legislation.

Exclusions:

Employees and contractors – you [will] have a separate contract in-place, usually your employee or contractor handbook – email HR@iwhotels.co.uk for more information.

LEFT INTENTIONALLY BLANK

4. What we collect from you

Data from a reservation or enquiry (via any channel):

All reservation data we collect and store about you is handled and stored by U.S Booking Services Limited trading as Freetobook – a copy of their privacy statement is from page 16. We remain jointly liable for your data, with Freetobook being the data storage facility.

If you make your reservation through a third-party booking site or agency, they may also store your data – for this we are not liable.

- Your full name, and the full names of your guests.
- Your identification documents (passport, driving licence etc) and those of your guests.
- Your email address(es) and telephone number(s).
- Demographic information – your home/billing postal code, address line(s), town/city, county and country – and your preferences and interests.
- Other information relevant to customer surveys and/or offers and newsletters.
- A token linked to your payment card (via Stripe).
- Dietary requirements of you and your guests, as applicable.
- Disabilities and other important health conditions, as applicable.
- Special requests – birthdays, anniversaries etc, as applicable.

We (may) need to collect the above information for business purposes only – to accommodate you and your requirements. Data may be stored by us digitally on Freetobook, or on paper in a secure location on our premises only.

CCTV:

- Video recording in place internally on our premises, as well as neighbouring – externally and adjacent – for the purposes of crime prevention, your safety, our protection and auditing of deliveries – including emergency exits, car parks, pavements, corridors, facilities, and public areas. We do not have cameras in private guest rooms/units nor inside bathroom or changing facilities.
- Audio and video recording in transaction locations – receptions and bars – for the reasons above as well as for auditing and fraud prevention.

As part of our PSOP / risk assessments, we monitor and record video in our swimming pools and spas for your safety.

Yellow signage is clearly displayed in locations where CCTV is being utilised by us; the reasons for use at each location, and how to contact us. You may become a data subject as an un-suspecting member of the public when passing outside our premises – your rights are covered under this policy also.

SECTION CONT'D ON PAGE 6

Registration:

We are required by law to collect details from all guests upon check-in. This is usually done online through our booking system provider Freetobook, though we reserve the right to ask you to complete this with pen and paper. We are required to provide this information to authorities (customs or border force officers) immediately upon request and without your knowledge.

We may keep a token linked to your payment card when you arrive, by way of a pre-authorisation – we will inform you and seek your permission first. We reserve the right to take a copy of your ID whilst you are occupying the accommodation.

Telephone call recordings and logs:

We reserve the right to record any calls made by us or to us – for training and auditing purposes. This therefore may include any information you give us verbally. If we are utilising call recording, this will always be announced to you at the start of the call. If you wish to decline the recording of your call, please disconnect the call and write to us instead.

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

Written correspondence (email and letters):

We reserve the right to store any information you provide us in written correspondence to contact or respond to you and to assist with your enquiry.

Internet enabled device data:

Our wired and wireless (Wi-Fi) networks store basic data about your device(s) when connected to our networks, which we use for internal diagnostic, for improvements and legal purposes only. At the data of this document, the data we collected includes:

- Local IP address
- Device MAC (or Wi-Fi) address
- Device hostname (e.g. Jon's iPhone)
- Connection time and history
- Access point connection and movement/handoff information
- DNS traffic data – including packets that have been blocked / flows blocked

Our chosen internet service providers are WightFibre Limited and British Telecommunications Plc. We cannot control the data our ISP may store our and your use of the internet.

SECTION CONT'D ON PAGE 7

Accident / incidents:

Any accidents or incidents that occur on the premises will be recorded along with any information you provide on the incident form – additionally this could be your date of birth, health conditions, nature of incident and/or your statement of event(s).

This may need to be shared with our insurers, [the] Health and Safety Executive under RIDDOR, or local or national authorities – see section 6.

Exclusions:

- We do not collect or process any special categories of personal data (including race or ethnicity, religious or philosophical beliefs, sexual orientation, political views, trade union membership, health, genetic or biometric data), nor do we collect any information about criminal convictions and offences.
- Employees are not covered by this policy – the use of CCTV, correspondence between you and us, call recording, computer/internet usage and accidents and incidents – information about how we control and manage your data can be found in your employee handbook.

LEFT INTENTIONALLY BLANK

5. How we keep your information safe:

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard the information we collect about you. This could include:

- Door locks (staged master key systems)
- Alarm systems
- Auditing logs
- Separate logins / user accounts for members of staff with access restricted as per our management structure
- Passwords changed every month and 2-step authentication
- Management structure (see below)

Management structure:

The board of directors and executive / senior management are permitted full unrestricted access to all levels of data. Heads of departments are permitted access only to data stored by and for their department. All other employees are permitted limited access supervised by their heads of departments. Outside contractors are permitted access on an ad-hoc basis as required with signed authorisation from a director or executive.

- Board of directors – Mr. N. J. Spyker, Mrs. J. Moorman, Mr. M. Moorman
- Executives / Senior management – Mr. D. Banks, Mrs. K. A. Banks, Miss. K. G. Moorman
- Heads of departments – Mrs V. Moorman (Reception), Mr. G. P. Banks (Estates & Plant), Mrs. V. Gough (Reservations), Mr. B. Norman (Bars), Mr. C. Finnis-Jones (Catering), Mrs. J. Gallop (Housekeeping)
- Other employees – Receptionists, Reservation Clerks, Bartenders, Hall Porters, Night Porters / Security, Waitstaff, Cleaners, Maintenance
- Third party contractors employed to conduct a task on our behalf – e.g. software developer, IT firm, or secure waste destructor

Reservations:

Only the lead guest/booker can make amendments or requests to an active reservation – by telephone, by email or any other channel. We will always ask you to confirm at least two pieces of your personal information to confirm it's you we're communicating with. No one else will be permitted access to amend your reservation or access your data.

We will only respond to emails regarding your reservation to the email address we hold for you.

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

SECTION CONT'D ON PAGE 9

CCTV and other computer systems:

CCTV recordings are kept for no longer than 31 days and then automatically overwritten. CCTV servers are kept in secure rooms with locked doors, or in a locked cabinet. All data on the hard drives are encrypted.

At the date of this policy, CCTV live monitoring and recordings are only accessible by two members of the executive / senior management team.

Only permitted and trained employees are permitted to use company computer and devices. Files servers are kept in a secure locked room with limited access – all data is encrypted and backed up regularly.

Our computers and servers 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.

At the date of this policy, network data is accessible by one member of the executive / senior management team.

To further keep your information safe, our websites and booking pages use SSL encryption, as indicated by the secure (padlock) symbol on the address bar of your chosen browser. You should not input any personal information into a site not displaying this symbol.

Incidents / accident reports:

Once completed by a member of our staff, a physical copy will be kept in the locked hotel office and at the company's registered office, as well as a [scanned] copy on the company's computer network.

Training and awareness:

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.

All departments are included in regular training session(s) surround data protection – at least annually. Regular email updates and flyers are sent out to employees.

Any new legislation, updates or recommendations are communicated to employees at the earliest opportunity (usually within seven days) facilitated by the data protection officer, executive / senior management team and/or heads of departments. Newly recruited members of our team are fully trained prior to handling your data.

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

Auditing means we are able to hold employees or contractors to account for malicious acts including, but not limited to, unlawful distribution and/or sharing of data.

6. Payment processing

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 / channel manager 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 issuer’s mobile app or by SMS text message.

Reservations made through a third-party agency or website (e.g. Booking.com) may collect payment direct from you and pass this onto us later. We are not liable for any payment details collected, stored or processed by third parties.

If we have processed payment directly, the descriptor on your bank account or card statement will read: ‘SANDRINGHAM HOTELS IOW’, ‘ISLE OF WIGHT HOTELS L’ ‘SANDRINGHAM HOTEL’ or ‘CALVERTS HOTEL’. If anything else shows, we have not processed your payment – the third-party will have their own payment processing statements.

Payments made to us in-person will be by completed on a card terminal by chip & PIN, contactless or NFC. We do not accept signature or swipe card payments as these carry a high risk of fraud. Our card terminals only store the last four digits of your card.

Groups bookings or said third-party agencies usually make payment to us by direct electronic bank transfer (BACS, Bank Giro Credit or Faster Payment) – in this event we do not hold any payment information for / about you, your organisation or your clients (our mutual guest). If you provide us with your payment card, you are covered by these terms also.

LEFT INTENTIONALLY BLANK

7. Sharing of your data

We will never share or disclose any information about you to unrelated or unnecessary persons internally within the company nor to any third party.

Internally (between departments):

We will share any dietary requirements with our catering team and waitstaff.

We will share any disabilities or important safety information about you with receptionists, night porters and housekeeping teams.

Externally (third parties):

We will share any disabilities or important safety information about you with authorities or fire personnel in the event of an emergency or fire alarm.

If we book your ferry travel for you, we will need to share a limited amount of your information to the ferry operators – your full name, your phone number and your vehicle registration with: Southampton Isle of Wight and South of England Royal Mail Steam Packet Company Limited trading as Red Funnel, or Hovertravel Limited. In this case the ferry operators also become controllers of your personal data.

We may be required by law to share information we hold/know about you to local or national authorities such as police forces, national crime agency, action fraud, border force or HMRC etc. upon request from them. This could include (as applicable):

- Your full name and the names of your guests
- Your contact details, including address
- CCTV video/audio footage whilst on or around our premises
- Dates of your reservation(s) and historic reservations
- Evidence of any criminal activity
- Receipts and invoices showing purchases and transactions
- Any other information provided on a registration form or accident / incident form

We will not make you aware of submissions we have legally had to make to any Government or Local Authority.

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, indicating so on the accident form which you will have access to and a copy of.

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

Any physical copies of your data stored at the end of our retention period are transported to or collected by a local confidential waste destruction company – see section 8.

Our transfer rights as outlined in section 11.

8. Retention periods

We are required to retain all transaction and reservation records – physical or digital – for six years as per the auditing requirements of His Majesty’s Revenue & Customs (HMRC) – this is the period which we retain your personal information.

Data stored within our booking system Freetobook is retained as per their own privacy / data protection policy.

A token linked to your payment card is stored until the departure date of your reservation via Freetobook and Stripe.

A pre-authorised payment is held for 0-3 working days preceding your departure date.

Physical (paper) copies of your information that we may hold are in a secure in-house facility; then collected by a local confidential waste destruction company to be destroyed, which is then certificated, with a certificate provided to us.

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, 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.

LEFT INTENTIONALLY BLANK

9. In the event of a 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.

LEFT INTENTIONALLY BLANK

10. Your rights – how you can control and access your information

Your rights, as well as our duties, are outlined under the EU's General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy is governed by the law and courts of England and Wales only; any other legislation does not apply to this policy.

Subject access request:

You have a right to a copy of your personal data we hold, along with any supplementary information. We will respond to you without delay and within one calendar month from our receipt of your subject access request; we are permitted to extend this to two months if your request is complex or if it involves multiple requests made by you. We reserve the right to refuse your request if an exemption or restriction applies, or if the request is manifestly unfounded or excessive – additionally we reserve the right to charge you a fee to cover our administration costs. The information / data we may hold about you for any period could include:

- All those listed under section 4.
- CCTV video and audio recordings
- Registration forms / photo ID collected from check-in
- Restaurant and bar orders
- Telephone notes made by reservations team
- Email and postal correspondence

To make this request, please do so by emailing [the] **DPO@iwhotels.co.uk** or writing to the 'Data Protection Officer' at the company's registered office address.

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

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

Please ensure you also read and understand our terms and conditions prior to submitting a subject access request – <https://isleofwight.info/Terms-Conditions.pdf>

Complaints and concerns (following a subject access request):

Should be made as soon as possible in writing to 'The Directors' at the company's registered office address.

After this point if we are unable to resolve this matter with you, you are permitted to contact the ICO whom we will work with and support their investigation.

LEFT INTENTIONALLY BLANK

11. Other important / regulatory information:

This contract is between you and us only. No other person or third party shall have any rights to enforce any of its terms, whether the Contracts (Rights of Third Parties) Act 1999 or otherwise.

We can transfer our rights and obligations outlined under this document to another organisation, but this will not affect your rights or our obligations under these terms and conditions. We will notify you if this happens (for example: sale of a business or re-structuring). You can't transfer your rights and obligations unless we agree this with you in writing.

Each of the clauses of these terms operates separately. If any court of relevant authority decides that any of them are unlawful or unenforceable, the remaining clauses will remain in full force and effect.

END

Freetobook Privacy Statement

Freetobook is booking software used by accommodation providers to enable their customers to make online bookings and manage those bookings. This document applies to the processing by freetobook of personal data collected by properties using freetobook online booking system in relation to the provision of accommodation by those properties.

Your personal data:

Properties using freetobook as their booking engine, collect and store information that you give when you make a booking. You are asked for your name, address, telephone number and email along with payment information and “the names of any guests travelling with you”. This may also include your IP address. This information is stored in the freetobook System in order to process your booking. You may be contacted by the Property you have booked with in relation to your booking.

Your data is also stored after you have stayed but will be kept no longer than necessary in order to comply with legal obligations and for properties to welcome your repeat business.

Data processed directly by third parties:

If you provide payment information, this will be processed directly by secure PCI Level 1 compliant payment gateway providers.

Joint controllers:

In the context of providing booking software to accommodation providers to facilitate online booking, freetobook and the accommodation provider shall together operate as joint data controllers for the processing of your personal data.

Security procedures:

In accordance with General Data Protection Regulation (GDPR), freetobook observes reasonable procedures to prevent unauthorised access and misuse of personal information. We use appropriate business systems and procedures to protect and safeguard any personal information given to us. We also use security procedures and technical and physical restrictions for accessing and using the personal information on our servers. Only authorised personnel are permitted to access personal information in the course of their work.

Control of your personal data:

You have the right to access data that is stored on behalf of properties taking bookings via freetobook system. You need to email or write to the property you booked with to request an overview of your personal data.

You can also contact the property you booked with on freetobook System if you believe that the personal information they have for you is incorrect, if you believe that they are no longer entitled to use your personal data or if you have any other questions about how your personal information is used or about the Privacy Statement. You need to email or write to the property you booked with.

Reviews:

You may also be asked to send feedback after your stay in order for the property to further improve their service. Your email address will be used for this purpose. If you complete a review it may be posted on the property website, facebook page, twitter or google plus. However, no identifying details will ever be attached to a review posting.

To Process your information as described above, we rely on the following legal bases:

Performance of a contract:

The storage of your information may be necessary to perform the contract that you have with the accommodation provider you are booking with.

Legitimate Interests:

We may use your information for our legitimate interests, such as for administrative, fraud detection and legal purposes.

Cookies:

A cookie is a small amount of data that is placed in the browser of your computer or on your mobile device. These cookies are used only to help you make a smooth booking and contain information like the date searched and language of booking. There is a difference between session cookies and persistent cookies. Session cookies will only exist until you close your browser. Persistent cookies have a longer lifespan and are not automatically deleted once you close your browser. We use persistent cookies in Google Analytics to analyse visitor traffic and behaviour.

By using freetobook website or proceeding with a booking you are consenting to the above use of cookies.

END