



Privacy Policy & Privacy Notice

Version date: 19 August 2023

Introduction

The Ostrich Inn Newland Limited and our affiliate companies (“**The Ostrich Inn**”, “**us**”, “**we**”) invest in and operate The Ostrich Inn in Newland Gloucestershire and we take data privacy and security very seriously.

In addition, we are also required to comply with the requirements of relevant privacy laws, including the General Data Protection Regulation (“GDPR”).

This Privacy Notice explains who we are, what data we collect from you, how we use personal data, and how you can exercise your rights.

Our details are below and if you have any questions about our use of your personal data, then please contact us.

Please note that this notice is for our engagement with persons other than our staff, to whom a separate notice applies.

Status of payment card data

We use the following systems for card payments, we do not store or retain your card details when these systems are used. The privacy terms for these systems can be found on the supplier’s website

- **SumUp** – the card readers we use with our till are provided by SumUp. Their privacy notice can be found here: <https://www.sumup.com/en-gb/general-privacy-policy/>
- **Stripe** – our on-line booking system uses Stripe to take card deposits and/or take payments for ‘no shows’. Their privacy notice can be found here: <https://stripe.com/en-gb/privacy>

What we collect and why we collect it

We will collect, process and retain information about you that you provide voluntarily, that we collect automatically and that we obtain from third party sources, such as your employer.

When you engage with us, we may ask you to provide personal information to us. The personal information we may collect about you includes:

- Identity and Contact Data: name and contact details (which may include phone, email, and social media identifier);
- Communications Data: Data shared with us over email or through our website or social media; and
- Commercial data to manage any payments that we are required to make to you.

When you visit our website, visit our offices or connect to our IT systems we may collect the following information automatically:

- technical Data: information that identifies persons and/or devices making use of our networks and systems, and usage and administrative information related to such use, for example attendance at online meetings and meeting chats;
- if you meet with us online and if it is recorded, then audio data may be retained; and
- our website and social media may keep records of pages visited and links clicked.

We will also from time to time obtain personal information about you from a third party source, such as your employer or recruiter, for the purpose of us being able to contact you.

Our processing purposes and the legal basis for them

Our reason for collecting the personal information set out above and the lawful basis on which we process that data depends on what the information is, why we collect it and what our relationship with you is.

We have set out a description of the ways we will use your personal information and which of the legal bases we rely on to do so in the list below.

Why we do this	On what basis do we process this data?	What sort of data does this apply to?
To fulfil any requests submitted via our website or social media	<ul style="list-style-type: none"> ▪ Necessary for our legitimate interests to respond to and/or engage with you ▪ Performance of any contract you have with us. 	<ul style="list-style-type: none"> ▪ Technical Data ▪ Contact Data
To protect you and other individuals	<ul style="list-style-type: none"> ▪ Necessary to protect your vital interests where your safety or health is at risk. 	<ul style="list-style-type: none"> ▪ Health Data ▪ Identity and Contact Data
To operate and manage our premises	<ul style="list-style-type: none"> ▪ Necessary for our legitimate interests to make our premises, including items such as guest wifi, available to you and to properly manage your visit ▪ Performance of a contract where your visit relates to your contractual relationship with us ▪ Necessary to comply with a legal obligation if we are required by law to obtain health data (for example if COVID-19 or similar controls apply). 	<ul style="list-style-type: none"> ▪ Technical Data ▪ Identity and Contact Data ▪ Image Data (CCTV) ▪ Health Data
To detect security	<ul style="list-style-type: none"> ▪ Necessary for our legitimate interests to protect our business from criminal 	<ul style="list-style-type: none"> ▪ Technical Data

Why we do this	On what basis do we process this data?	What sort of data does this apply to?
breaches, breaches of policy or procedure or identify unlawful activity	activity or breaches of policy that impact us physically or logically (for example cyber-crime attempts).	<ul style="list-style-type: none"> ▪ Image Data
To understand (including by using cookies or other technical tracking technology) how you interact with our website and social media, and for data analytics so we can improve our use of these means of communication	<ul style="list-style-type: none"> ▪ Necessary for our legitimate interests to improve the quality and relevance of our website and social media. ▪ Please note that technologies such as cookies may be subject to separate regulation and, where required by those regulations, you may be able to opt out of their use. 	<ul style="list-style-type: none"> ▪ Technical Data
To manage our contract with you and deliver our services	<ul style="list-style-type: none"> ▪ Performance of a contract with you. 	<ul style="list-style-type: none"> ▪ Identity and Contact Data ▪ Technical Data ▪ Financial Data ▪ Audio Data
To send promotional and marketing content	<ul style="list-style-type: none"> ▪ Necessary for our legitimate interests to promote our services to you (where consent is not required) ▪ Where consent is required, with your consent. 	<ul style="list-style-type: none"> ▪ Contact Data
To share information with law enforcement and others, in circumstances where this is necessary to protect you, our staff, our business or our facilities	<ul style="list-style-type: none"> ▪ Necessary to protect vital interests where there is a risk of harmful conduct or a person's safety is at risk. ▪ Necessary for our legitimate interests to protect you, our staff, our business and facilities. ▪ Where we are required by relevant law to share the information 	<ul style="list-style-type: none"> ▪ Technical Data ▪ Identity and Contact Data ▪ Image Data

If we ask you to provide personal data to comply with a legal requirement or to perform a contact with you, we will make this clear at the relevant time and confirm if in those circumstances you must provide the data to us.

Sometimes, we will use your data to pursue our legitimate interests in a way which is reasonable for you to expect as part of running our business and which does not materially affect your rights and freedoms. We have set out below what our legitimate interests are.

We take measures to ensure that your personal data is kept secure and to limit our processing activities to what is necessary for our legitimate interests.

We may also sometimes have a legal obligation to collect personal data from you or may need the personal data to protect your vital interests or those of another person (for example if we need to contact the emergency services if there is an incident or accident at our premises.)

You also have the right to object to processing that we undertake for our legitimate interests, see further below.

Who will process your personal data and where will it be processed?

Your personal data may be processed by us and by the third parties who we are entitled to disclose your personal data to (see further below).

Your personal data may be transferred to and processed in countries other than the United Kingdom. This includes:

- services hosted by third party suppliers in data centres across UK, European Economic Area (EEA) and USA
- our group and affiliate companies that operate in the USA, the UK and the EEA

Where we do transfer your personal data outside of the UK to a country which is not subject to an adequacy decision, we will take appropriate safeguards to require that your personal data will remain protected in accordance with this Privacy Notice. The safeguards we use are the European Commission's Standard Contractual Clauses for transfers of personal data to third parties, including the UK Addendum. These require those recipients to protect personal data they process from the UK in accordance with UK data protection law.

Who may we share your personal data with?

We may disclose your personal data to the following categories of recipients:

- to our group and affiliate companies, who provide data processing services to us or who process personal data for the purposes set out in this Privacy Notice
- to our tenants, suppliers, contractors, service providers & partners who provide data processing services to us, or who process personal data for the purposes set out in this Privacy Notice or notified to you when we collect your personal data. This includes the following types of third parties:
 - security service providers who provide security services in relation to our premises and our operations

- facilities management and other outsourced services providers who contract with to provide services to us
- service companies who provide, manage or support of our IT infrastructure and services
- insurers who insure our premises, business and people
- to any relevant law enforcement body, regulatory or government body, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person
- to an actual or potential buyer (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business or that of our group companies or affiliates, provided that we inform the buyer that it may not your personal data other than for the purposes of assessing the proposed transaction and/or for any other purposes that are set out in this notice
- to any other person with your consent to the disclosure.

How do we keep your personal data secure?

We use appropriate technical and organisational measures to protect the personal data that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal data. Specific measures we use include: encryption; anonymization (where practicable); and access control to systems.

How long will we retain your data?

We will retain personal data where we have continuing legitimate business need to do so. When we no longer need to process your personal data, we will either delete or anonymise it or, if this is not possible (for example, because your personal data is stored in archives), then we will securely store your personal data until deletion is possible.

We apply the following retention periods for personal data:

- identity and contact details - until your access to our premises is ended;
- Security CCTV images - for the retention period of the system which for security CCTV does not exceed 90 days (unless an incident occurs - such as a suspected crime or security breach - which requires us to keep footage and images relevant to the incident for a longer period of time).
- information that identifies persons and/or devices making use of The Ostrich Inn networks - no longer than 9 years;
- contact details for sales and marketing - until you unsubscribe/object/opt-out from our sales and marketing information. If you do so we will retain limited information sufficient to enable us to ensure that you remain unsubscribed.

Site monitoring camera (time lapse) images are at a resolution/distance where individuals are impractical or impossible to identify and which we do not regard as personal information, but it is retained no longer than 9 years.

How to access your personal information or make a request in relation to other rights.

Requests may be made in writing, see below for how to contact us. All requests will be recorded, and, as we cannot provide information other than to the person that it relates to, you may need to provide information to verify your identity and enable us to locate the information. Please provide:

- Full name & address
- An indication of what information you are requesting to enable us to locate this in an efficient manner.

Examples of acceptable identity evidence are listed below. We require, where applicable, two items from List A and one from List B.

- List A: ID documents, examples are: Passport Driving license
- List B: Proof of address, examples are: Bank statement, Utility bill

Updates

We may update this Privacy Notice from time to time in response to changing legal, technical or business requirements. Updates will be placed on our website and dated on their date of issue.

Data controller

The data controller of the personal data to which this Privacy Notice applies is The Ostrich Inn Newland Limited.

Contact us

If you have any questions or concerns about our use of your personal data, please contact us using the following details:

E-mail enquiries@theostrichinn.com or write to the directors at The Ostrich Inn Newland Limited, Newland, Gloucestershire, GL16 8NP

Document ends.