COTTESMORE
HOTEL GOLF & COUNTRY CLUB

Data Privacy Policy

GDPR

(General Data Protection Regulation)

The GDPR legislation came into force on 25th May 2018 and replaces the 1995 Data Protection Directive. GDPR governs personal data information – how it's captured and who it's shared with.

Personal Data Stored and Used with Consent

Achieving GDPR compliance is a company wide goal at Cottesmore. All data will be handled for the purpose for which it was entrusted. We aim to build a database of those who have given explicit consent to receive our company newsletters and offers.

Cottesmore will never sell your data to any third party.

How does Cottesmore collect data?

- **Members.** On joining the club personal data is collected for the purposes of your membership, i.e. internal communications, newsletters, etc.
- **Visitors.** Personal data is stored for the purposes of the visit only, i.e. hotel confirmation, conference & event planning, beauty treatment booking confirmation. Consent must be given for wider use.
- **Online.** Via various online marketing platforms data is provided at the discretion of the individual for specific purposes, i.e. general newsletter, golf offers etc.

Where is your data stored?

Cottesmore uses four separate software systems for operational purposes.

- **ESP, Shortcuts. Both server based.**
- **Clock PMS – Cloud based on the EU Amazon server. (GDPR compliant)**

Cottesmore's marketing database is stored on our email database account. All email addresses held on the database have been submitted with consent for the purposes of receiving our newsletter and offers.

All four forms of software are protected by username and password to ensure data is only accessed by those authorised to handle it. Additionally, user rights within each system govern access from an internal perspective.

How does Cottesmore manage stored data?

A regular review process or data purge is conducted across the four operational software systems (ESP, Clock, Shortcuts, email database) that hold personal data. If there is no requirement to hold the data based on the original purpose for which it was retained, i.e. a one off accommodation booking or salon treatment, it will be reviewed for deleting.

It is the duty of the General Manager, as the Data Protection Officer, to ensure that the data privacy policy is adhered to.

How do I access my data?

We aim to conduct a highly transparent data policy whereby anyone may contact the General Manager on manager@cottesmoregolf.co.uk to verify the status of any information held. It may be edited or deleted at any time. In line with GDPR regulations this will completed within 30 days.

Young Person's data rights.

The General Data Protection Regulation proposes introducing 16 as the minimum age at which a person can join an online service without the consent of their parents. Data of those under the age of 16 will not be stored without the consent from their parents.

In the event of a data breach?

If the circumstances arise where our security measures are breached and an unlawful access to personal data is achieved we are legally required to contact those involved within 72 hours. An investigation will be launched by the Data Protection Officer immediately into the cause of the breach and how to prevent it reoccurring.

CCTV.

Cottesmore operates a CCTV system for security purposes and for the protection of our employees. All security cameras in operation permanently record onto a server at Cottesmore held on a secure network. The recorded footage is held for 14 days before it is automatically recorded over. Any recorded footage will be made available on request.

Card Payment Systems.

Card payment transactions are regulated under the Payment Card Industry Data Security Standard (PCI DSS) to which Cottesmore is highly committed thoroughly quarterly compliance schedules to protect card data.

PCI DSS is the worldwide Payment Card Industry Data Security Standard that was set up to help businesses process card payments securely and reduce card fraud. This is achieved through enforcing tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

The payment standard has requirements which fall into the six categories below:

1.) Build and Maintain a Secure Network

2.) Protect Cardholder Data

3.) Maintain a Vulnerability Management Program

4.) Implement Strong Access Control Measures

5.) Regularly Monitor and Test Networks

6.) Maintain an Information Security Policy

Card data is only used for the intended purpose for which it was submitted. The card data is then destroyed or automatically deleted following its intended use.

Data Protection Officer.

Johnny Porter – General Manager

manager@cottesmoregolf.co.uk