Rosewyn Farmhouse Limited

DATA PROTECTION POLICIES

Introduction

1. This information is provided in compliance with the EU General Data Protection Regulations (GDPR).
2. The Policies relate to Rosewyn Farmhouse Limited (the legal entity) and the directors of that company (the directors).
3. The directors consider that the security of guest personal data of a matter of the highest importance. This is due to the breadth and scope of the data and its sensitivity.
4. It has long been a principle that guest information is not disclosed by any means without the authority of the guest. The fact that data is now held in many differing forms does not change the underlying principle.
5. This document should be read alongside this company's Privacy Notice.

Data holding policy

1. We will only hold data that is required to fulfil our contractual obligations to our guests and to conform with the legal and professional framework that we are required to adhere to.
2. We will not host guests who fail to provide us with all of the necessary data that we require in order to comply with our obligations.
3. The act of providing data to us with a request to book a self catering letting and will be taken by us as clear consent.
4. The act of booking a self catering letting will provide the guest with the opportunity to check the data that we hold on them.
5. In our view data is currently held more securely on online servers and we endeavour to move more towards this position, whilst being mindful of the fact that in certain cases it is helpful to retain paper records.

6. Where data is not to be transmitted to a body in accordance with the Law, we will not disclose ant data to any person, or body, without the prior written consent of the guest, and this includes the acknowledgment that we host the guest. This also includes spoken communication.
7. HMRC are, in certain circumstances, permitted enquire into the host's tax affairs retrospectively for 20 years. We will hold guest data with that in mind, but in most cases 7 years will be considered adequate. It will be necessary for us to inform the guest of this obligation in the event that the guest wishes to exercise certain GDPR rights.

Physical security policy

1. Data that is held in files comprising paper records, and data that is held on the hard drives of computers are kept in our secure office, which is locked at all times when a director is not present.
2. Backup hard drives are retained in a locked safe.
3. Paper records are scanned into pdf files from time to time depending on the need to refer to the guests history easily. Once scanned the original paper records are locked away until they are burned in the presence of a director, or where not sensitive, shedded by a member of staff.

Digital security policy

1. Data that is held on the company's computers and backup hard drives (data at rest) is protected by a number of methods, including:
   - Hard drive encryption
   - Boundary Firewall protection
   - Endpoint Firewall protection
   - Advanced Heuristics Antivirus Scanning (Eset Endpoint Antivirus)
   - Hourly Recovery enabled backups to encrypted hard drives (Carbon Copy Cloner)
   - Weekly (minimum) Fire backups to encrypted hard drives held securely away from the office (Carbon Copy Cloner)

- Complex password protection for all endpoints and software (1Password)
- UPS standby power protection
- Wifi disabled network
- Removable data devices blocked (Eset Endpoint Antivirus)

2. Data that is held on online servers is considered to be as secure as we can make it. The follow attributes apply to online software:
    - It is commercially available and therefore subject to GDPR
    - It is approved by HMRC
    - It is industry standard
    - It is held on servers within the EU

Hardware policy

1. In order to achieve the highest standards of data protection we believe that our use of hardware is an essential part of providing a secure and reliable computer system. Accordingly, it is our policy to use the following suppliers equipment:
    - Computers: Apple
    - Network switches: Netgear
    - Printers: HP and Epson
    - Scanners: Epson
    - SSD Drives: Crucial

Operating systems policy

1. All computers will use the same OSX Operating System (currently Ventura 13.4). Auto updates are enabled. Windows OS will not be used on Mac PCs, or connected to the network.

Data in transit policy

1. Data in transit around the Network is protected by the system already described in the Digital security policy. Other data in transit can arise in the use of emails. We use Postbox as commercial Email software and this includes the ability to encrypt messages that include personal data. We will encrypt emails where personal data is included.

Application software policy

1. It is our policy to move more and more software to online systems.

CPS 310523