PRIVACY POLICY

This privacy policy sets out the privacy practices for:

MILLETS FARM CENTRE LTD **Company number 09187968**

MILLETS RESTAURANT LTD **Company number 09747118**

MILLETS PLAY BARN LTD **Company number 10612329**

Trading Address: Millets Farm Centre, Frilford, Nr Abingdon, OX13 5HB

Registered office: 38-42 Newport St, Swindon, SN1 3DR

Websites: www.milletsfarmcentre.com and www.sproutsplaybarn.com

Email: enquiries@milletsfarmcentre.com

In order to provide services to our customers we will need to collect and process personal information. We are committed to protecting the privacy and security of personal information in accordance with the applicable data protection laws including the General Data Protection Regulation.

This privacy policy describes how we collect and use personal information.

We will always comply with the data protection principles as follows:

- Fairly and lawfully collecting and processing data
- Providing information about the data which is held and how it is used
- Using data only for the purpose for which it is collected
- Keeping data accurate and up to date and ensuring it is kept for no longer than necessary
- Deleting or anonymising data once the purpose for collection is met
- Implementing appropriate security measures to ensure data is kept safe
- Providing the right to access, correct and erase data

If you have any questions about this policy or the website, or about how we use and process your personal information please do not hesitate to contact us by email. This policy will be reviewed and updated on a regular basis as required.

CONTENTS:

1) CUSTOMER DETAILS:

Why do we need them?

1. Customer name and contact details will be required when orders are placed for products, including gift vouchers, or services such as a party or a private function. Taking contact details ensures if we have any queries about the order we have the means to clarify with the customer to ensure we deliver the service to the highest standard.
2. Customer details may be taken if they were to enter an onsite competition in order to contact them should they win.
3. Customer details may be left if they were to complete a customer comment card and requested feedback from Millets Management.
4. Customer details will be taken in the case of an accident or incident onsite which needs recording for legal and insurance purposes.
5. Customer details will be received should they contact us via any of the milletsfarmcentre.com email addresses promoted on our website or social media platforms.
6. Customer details are stored for online marketing email communications where they have accepted marketing at the point of purchasing a ticket, product or booking a table via our website.
7. Customer details are stored for online marketing email communication where they have signed up to receive our e-newsletter via our website.

How do we store them?

All customer details should be stored safely until the point at which the product or service has been delivered. Such safe places include:

- In appropriate books or folders that can be accessed by the required members of the department or senior management only.
- In sealed envelopes if in transit.
- On prep sheets stored within a locked office/room/filing cabinet.
- On forms that are delivered directly to Management who would then store them within a locked office/room/filing cabinet.
- Posted into a locked boxed, only accessible by an appropriate Millets team member who would then process them securely.
- On a Millets email address held on a password protected computer.
- On excel spreadsheets on Millets password protect computers.
- Within password protected software such as Digitickets, Trana and MailChimp provided they have robust GDPR processes.

Unauthorised places include:

- Anywhere within view of the general public.
- On a white board or wall planner that can be viewed by anybody passing.
- On a white board/lying on a desk in an office that reps/trades people/non-Millets employees may be invited into.
- On non-Millets email accounts, laptops, tablets, phones or any other data storing device.

Where a payment needs to be taken over the phone no customer card details should ever be written down but entered directly into the payment terminal.

Sharing Customer Data

1. Customer details may need to be shared between different member of the Millets team in order to properly deliver a service or deal with a query/incident. Customer details should be shared on a "need to know" basis only and should always be done so securely.
2. Sharing customer details with regulatory bodies such as Environmental Health will be carried out when legally required.
3. Sharing customer details with our insurers, accountants and lawyers will be carried out as required to process claims and during account auditing processes.
4. Customer details will only be used for Marketing purposes where consent has been given and an un subscribe option will always be available. Our customer e-newsletters will be sent using Mail Chimp software.
5. Customer details will be shared with online payment providers, Sage Pay or World Pay when purchasing tickets or products online.
6. Customer details will be shared with Trana eCommerce Ltd when purchasing products via the Millets Farm Online Shop.

7. Customers details will be shared with Digitickets when purchasing tickets, parties or boking tables via the Millets Farm Centre or Sprout Play Barn websites.

How long do we store them?

All customer details should be disposed of securely 1 month after the product/service has been delivered successfully. Secure disposal methods include:

- Tearing out pages of diaries and shredding.
- Shredding loose paper.
- Deleting emails and e-documents.
- Blanking out customer details if order details are required for analysis purposes at a later date.
- Anonymising electronically on Digitickets with the exception of email addresses where marketing has been accepted. Note all details will be retained where the customer has chosen to set up and account for future use, until the account has been dormant for 2 years at which point it will be anonymised.

If the order has been placed on behalf of another business the contact details of that business may be retained but the name of the individual contact will be removed.

2) EMPLOYEE DETAILS:

Why do we need them?

1. Employee personal details are required within HR to ensure they are legally allowed to be employed within the UK and to enable us to communicate with them regarding their employment at Millets.
2. Employee personal details and bank details are needed by Payroll to allow them to be paid for the work they complete and to submit information to HMRC and NEST pensions.
3. Employee contact details are required at a department level to communicate the shifts they are expected to work.
4. Employee email addresses are used to keep them updated with staff and site news.
5. Employee email addresses are used to provide them with employee discounts via Perkbox.
6. Employee names will be used in written documents and communication between management/colleagues on a day to basis to allow for the smooth running of the business.
7. Employee health and next of kin details are required in case of an emergency.

How do we store them?

All employee details should be stored safely for the duration of their employment. Such safe places include:

- Names and contact numbers only in appropriate books or folders stored in drawers or cupboards that can be accessed by the required members of the department or senior management only.
- On forms that are delivered directly to Management in a sealed envelope who would then store them within a locked office/filing cabinet.
- On a Millets password protected computer.
- Within password protected software such as Perkbox, Mailchimp, SAGE, Natwest Bankline, Bodet, Findmyshift, NEST.

Unauthorised places include:

- Anywhere within view of the general public.
- On a white board or wall planner that can be viewed by anybody passing.
- On a white board/lying on a desk in an office that reps/trades people/non-Millets employees may be invited into.
- On non-Millets email accounts, laptops, tablets, phones or any other data storing device.

Sharing Employee Data

1. Employee details may need to be shared between different member of the Millets team on a "need to know" basis only and should always be done so securely.
2. Sharing employee details with regulatory bodies such as HMRC will be carried out when legally required.
3. Sharing employee details with our insurers, accountants and lawyers will be carried out if required to process claims, during account auditing processes and for employment law support.
4. Employee details will be used for email communication purposes and an un subscribe option will always be available. Our staff e-newsletters will be sent using Mail Chimp software.
5. Employee details will be provided to Perkbox on completion of probationary period to allow the staff member access to employee offers and discounts unless requested otherwise.
6. Employee details will be shared with NEST pension provider if auto enrolment criteria is met. The Employee will then be responsible for opting out of the scheme if desired.
7. Employees details will need to be shared with training providers for any employee required to attend training courses or undertake a workplace NVQ.

How long do we store them?

Employee details should be disposed of securely at a department level as soon as the individual ceases to work at Millets Farm Centre. Secure disposal methods include:

- Tearing out pages of diaries and shredding
- Shredding loose paper
- Deleting emails
- Blanking out details in diaries
- Deleting details from software such as Perkbox, Mailchimp, Findmyshift, Bodet

Employee details will be kept by HR and Payroll for at least 7 years after the individual cease to work at Millets Farm Centre as is legally required for accounting purposes. These details may be archived.

IMPORTANT NOTE

Staff contact details should not be stored in personal mobile phones for work purposes.

Colleagues may have each other's contact details for personal reasons provided that information has been obtained on a personal basis, not through the data collection required for employment purposes.

Employees should not have managers personal mobile numbers. They should use work contact details to communicate with their managers i.e. the department phone number, Millets email addresses or Findmyshift messenger.

3) EXHIBITOR DETAILS:

Why do we need them?

Exhibitor name and contact details will be required for the running of events on site. Keeping details enables us to keep in contact with exhibitors in the run up to the event.

How do we store them?

- All exhibitor details should be stored safely until the event has been delivered, and unless the exhibitor gives written consent to be contacted with reference future events.
- The details will be stored both electronically, on Millets password protected computers and within password protected software such as ACT, and in paper form in locked offices.
- Exhibitor details will only be shared between members of the Events Team and Accounting.

4) COMPUTER MANAGEMENT:

- All computers should be password protected.
- All computers should have different passwords.
- All software that stores customer or employee personal data should be password protected.
- All software that stores customer or employee personal data should have different passwords.
- All passwords should only be given to the people who need to know them to complete their job role successfully.
- A password should be changed whenever an employee who knows the password leaves the company.
- A master sheet of all passwords should be kept by senior management and any changes to passwords reported immediately.
- When leaving your work space all computers or password protected software should be logged out of beforehand.

5) ENVIRONMENT MANAGEMENT:

- Any space containing sensitive personal information i.e. anything more than name and contact details should be locked with a key or code lock.
- All code locks should have different codes.
- Codes and keys should only be given to the people who need to know them to complete their job role successfully.
- Keys should be returned whenever an employee leaves the company, and locks changed if this has not been possible.
- Code locks should be changed whenever an employee who knows the code leaves the company.
- A master sheet of all codes should be kept by senior management and any changes to codes reported immediately.
- All spare keys should be sorted securely by Senior Management.

6) HOME WORKING:

- Using customer or employee personal data whilst working at home should be completed with the permission of senior management only.
- Work at home may be completed on company password protected laptops, tablets or phones only.
- When leaving your work all computers or password protected software should be logged out of beforehand.
- No customer or employee personal data should be removed from company devices or stored on personal devices.

- No paper records of customer or employee personal data should be removed from your place of work as sufficient safe storage will not be available in transit or in the home.

7) CCTV:

CCTV is used in some public areas to monitor and prevent antisocial behaviour and theft. Images will be recorded and stored for up to one month on a password protected computer in case they need to referred back to. Printed images of members of the public who have displayed anti-social behaviour or where there is photographic evidence of theft may be shared amongst Millets Employees for identification purposes in the future and will then be disposed of securely.

8) PROMOTIONAL IMAGES/VIDEOS:

Pictures and videos will be used in printed promotional materials, on our websites and as part of our social media marketing strategy. These pictures and videos may contain members of the public or employees. Each individual will be asked if they are happy to be included in such an image/video prior to it being taken and will be asked to sign a model release form giving consent for the future use of their image. Should they change their mind at a later date the image will be deleted from our library and will not be used in any future promotional materials. Any printed promotional materials that already exist will not be destroyed as consent was given at the time of printing but further print runs will not be carried out without removal of the image first.

9) COOKIES:

Our websites use cookies to better the users experience while visiting the website. Where applicable this website uses a cookie control system allowing the user on their first visit to the website to allow or disallow the use of cookies on their computer/device. This complies with recent legislation requirements for websites to obtain explicit consent from users before leaving behind or reading files such as cookies on a user's computer/device.

Cookies are small files saved to the user's computer hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server, to provide the users with a tailored experience within this website.

Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers' hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors.

This website uses tracking software to monitor its visitors to better understand how they use it. This software is provided by Google Analytics which uses cookies to track visitor usage. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information. You can read Google's privacy policy here for further information www.google.com/privacy.html

10) EMAIL NEWSLETTERS:

We operate an email newsletter program, used to inform subscribers about products and services supplied by this website. Users can subscribe through an online automated process should they wish to do so but do so at their own discretion. Some subscriptions may be manually processed through prior written agreement with the user.

Email marketing campaigns contain tracking facilities within the actual email. Subscriber activity is tracked and stored in a database for future analysis and evaluation. Such tracked activity may include; the opening of emails, forwarding of emails, the clicking of links within the email content, times, dates and frequency of activity [this is by no means a comprehensive list]. This information is used to refine future email campaigns and supply the user with more relevant content based around their activity.

In compliance with UK Spam Laws and the Privacy and Electronic Communications Regulations 2003 subscribers are given the opportunity to unsubscribe at any time through an automated system. This process is detailed at the footer of each email campaign.

Personal details are processed in accordance with the GDPR and as outlined earlier in this Privacy Policy.

11) EXTERNAL LINKS:

Our website only looks to include quality, safe and relevant external links, however users are advised to adopt a policy of caution before clicking any external web links mentioned throughout this website. (External links are clickable text/banner/image links to other websites)

We cannot guarantee or verify the contents of any externally linked website despite their best efforts. Users should therefore note they click on external links at their own risk and this website and its owners cannot be held liable for any damages or implications caused by visiting any external links mentioned.

12)SOCIAL MEDIA PLATFORMS:

Communication, engagement and actions taken through external social media platforms that we participate on are custom to the terms and conditions as well as the privacy policies held with each social media platform respectively.

Users are advised to use social media platforms wisely and communicate/engage upon them with due care and caution in regard to their own privacy and personal details. This website, nor its owners, will never ask for personal or sensitive information through social media platforms and encourage users wishing to discuss sensitive details to contact them through private messaging communication channels or via primary communication channels such as by telephone or email.

This website may use social sharing buttons which help share web content directly from web pages to the social media platform in question. Users are advised before using such social sharing buttons that they do so at their own discretion and note that the social media platform may track your request to share a web page respectively through your social media platform account.

13)IMPLEMENTATION:

All employees will receive the appropriate level of GDPR training to suit their individual role during their induction process at the start of their employment. Management staff will supervise and monitor junior staff members in their ongoing handling of personal data.

If you have any concerns or complaints about our privacy activities you can contact us on enquiries@milletsfarmcentre.com.

You can also contact the Information Commissioner's Office on 0303 123 1113.

Policy Updated May 2018