# Bambino Ltd

## Data Protection, Security and Privacy policy

| Version | Date | Author | Comments |
|---|---|---|---|
| 1.0 | 20/04/17 | Bambino Ltd | Initial release and adoption of policy |
| 2.0 | 02/03/18 | Sharon | Update with reference to new GDPR to include purposes of the processing, retention periods and right to withdraw consent. |
| 3.0 | 07/11/2018 | Sharon | Removal of sections referring to Employees' Data. This now forms part of the newly-created Data Privacy Notice for Employees. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Introduction

The purpose of this policy is to ensure compliance with The General Data Protection Regulation May 2018. The Company's Data Protection Officer is Sharon Peach and she can be contacted through the nursery manager.

If you want to know what information we collect and hold about you, please write to us at: Bambino Ltd, Tallowfoot, Naseby Road, Clipston, LE16 9GL

Bambino Ltd is the data controller of your Information for the purposes of the General Data Protection Regulation 2018.

With regard to employees, a serious breach of data protection is a disciplinary offence and will be dealt with under the Company's disciplinary procedure. If you access another employee's personnel records without authority, this constitutes a gross misconduct offence and could lead to your summary dismissal.

## The data protection principles

Personal data must be:

- Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the employee has given their consent to the processing, or the processing is necessary for Legal Compliance. Sensitive personal data may only be processed with the explicit consent of the individual.

- Obtained only for one or more specified and lawful purposes, and must not be processed in any manner incompatible with those purposes.

- Adequate, relevant and not excessive in relation to the purposes for which it is processed.

- Accurate and, where necessary, kept up-to-date.

- Not kept for longer than is necessary. The Company will keep personnel files for two years after an employee has left the Company's employment. Different categories of data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data which the Company does not need to hold for a particular period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

- Secure. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised employees have access to these files. Files will not be removed from their normal place of storage without good reason. Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked filing cabinets. Data held on computer is also stored confidentially by means of password protection, encryption or coding and again only the above employees have access to that data. The Company has network back-up procedures to ensure that data on computer cannot be accidentally lost or destroyed.

## Employees' obligations in relation to personal information

You must ensure you comply with the following guidelines at all times:

- Do not give out confidential personal information. In particular, it should not be given to someone, either accidentally or otherwise, from the same family or to any other unauthorised third party unless the data subject has given their explicit prior consent to this.
- Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.
- If you receive a request for personal information about another employee, you should forward this to the Data Protection Officer, who will be responsible for dealing with such requests.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another employee's records without authority as this will be treated as gross misconduct and it is a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable you to carry out your job duties and has been authorised by your manager.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.

## Parental consent to personal information being held

Parents can see and contribute to all the records that are kept on their child. However, we must adhere to data protection laws and comply with our Legal Obligations. Where relevant, this includes any guidance from the relevant agencies for child protection.

Parents have the right to ask us to stop processing personal data in relation to our service. However, this may stop us delivering a service to you. Where possible, we will do as you ask, but we may need to hold or process personal data to comply with a legal requirement. If you find that the personal data that we hold is no longer accurate, you have the right to have this corrected.

All parent, child and staff information is stored securely according to the requirements of data protection registration including addresses, phone numbers, permissions, certificates and photographic images. We will ensure that staff understand the need to protect the privacy of the children in their care as well as the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality.

The nursery's records and documentation are kept and stored in accordance with minimum legal archiving requirements. We currently archive statutory records

according to legal criteria – eg financial data such as fees paid by you is kept for at least 7 years and data surrounding accidents for 21 years and three months.

In the case of non-legal information eg email addresses or opting in to a newsletter, the data is destroyed or deleted immediately an individual withdraws consent.

## The personal information we collect from parents

We may collect personal information about you when you:

- ask about our service
- register a child with us
- sign up for showrounds, job interviews or newsletters
- apply to work for us
- become an employee
- telephone, write, contact us online or text us or otherwise provide us with your personal information.

This can include information such as your name, communication preferences, email address, postal address, IP address, telephone number, mobile number, date of birth or National Insurance number.

We may also hold personal/sensitive personal information in connection with our legal duties, for example who has Parental Responsibility for a child and also in connection with our financial obligations, such as the name of your employer if you pay your fees by Childcare Vouchers. No debit or credit card details are ever retained beyond the time taken to process a payment.

## How Do We Use the Information from parents/carers?

We use your Information in the following ways:

- to ensure that content from our website is presented in the most effective and efficient manner for you and your computer;
- to allow you to register and request information where you choose to do so;
- to notify you about changes to our service;
- in accordance with legal requirements at the point of Registration or other contact;
- to send you relevant information eg your nursery invoice, nursery newsletter or updates on your child's development.

We may pass your Information to third party organisations only:

- if we buy or sell any business or assets in which case we may disclose your Information to the seller or buyer of such business or assets;
- if we are under a duty to disclose or share your personal data to comply with any legal obligation or in order to enforce or apply our terms and conditions and other agreements or protect the rights, property, or safety of our customers, or others. This includes exchanging information with other companies and organisations for debt recovery.

## Data in Transit

There may be occasions when it is necessary for sensitive and personal data to be taken outside of the office e.g. if a member of staff is asked to attend a case

conference in a child protection issue. This includes data in all formats including but not limited to paper or electronic storage (PC's tablets, laptops and removable storage media i.e. USB memory sticks or any form of networking equipment). All employees are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data taken outside of the office is secure.

It is not possible to be prescriptive in this policy and procedure as to the action which should be taken to ensure security as there may be a number of different situations where data may be taken out of the office. It will be necessary for each individual taking data out of the office to assess the security measures needed for every situation and make considered judgements in terms of how they handle data whilst delivering their service and if in any doubt seek support from their line manager.

Any data loss must be reported immediately to the nursery manager who will assess the situation and impact and agree the necessary action with the Data Protection Officer.

## Accepting card payments

We use card machines as a portal for parents wishing to pay their fees by credit or debit card. We keep a list of such devices including:

- Make, model of device
- Location of device (for example, the address of the site or facility where the device is located)
- Device serial number or other method of unique identification

Staff authorised to use the card machines are responsible for the security of cardholder data. Before each use, staff must periodically inspect the devices to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device.)

***Note:*** *Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently coloured casing, or changes to the serial number or other external markings.*

In order to limit the risk of a security breach, such staff must:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behaviour and indications of device tampering or substitution to appropriate personnel (for example, to a manager or Sharon Peach).

In order to protect personal and financial data, we adhere to the following:

- Electronic lists of customer's credit card numbers should not be retained. Credit card information should only be accepted online, by telephone, or in person. This information should not be accepted via email.
- Only essential information is stored. We do not store the Card Verification Code (CVC) or users' PINs.
- Credit card information is only be retained for the time needed to process, after which time it is destroyed.

## Cookies

Bambino Ltd is committed to protecting any data (anonymous or otherwise) that we may collect about individuals online. None of the cookies used collect any personal data other than the IP address of web connections. By continuing to use our website (through any device) you agree with this Cookies Policy. We reserve the right to make changes to our Cookies Policy & confirm that any such changes shall appear here and become effective immediately. Data is retained for Google Analytics for 26 months.

## What if I don't want to accept cookies?

If you wish to restrict or block the cookies which are set by any website - including Bambino Ltd, you should do this through the browser settings for each browser you use, on each device you use to access the Internet. You can also allow cookies from specific websites by making them "trusted websites" in your Internet browser. For more information on how to do this please refer to www.allaboutcookies.org which explains cookies more fully and how you can manage, restrict, block or accept cookies within all popular web browsers (Internet Explorer, Google Chrome, Firefox and Safari).

Z

| Signed on behalf of the nursery | Print Name | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |