Bambino Ltd

Data Protection and Security policy

Version	Date	Author	Comments
1.0	20/04/17	Bambino Ltd	Initial release and adoption of policy

Introduction

The purpose of this policy is to ensure you do not breach The Data Protection Act 1998. If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the Company's Data Protection Officer (Sharon Peach).

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 his consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the employee and consists of information relating to:

Race or ethnic origin.
Political opinions and trade union membership.
Religious or other beliefs.
Physical or mental health or condition.
Sexual life.
Criminal offences, both committed and alleged.

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. If your personal information changes, for example you change address, you must inform your line manager as soon as practicable so that the Company's records can be updated

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 decides it 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.

Processed in accordance with the rights of employees under the Act.

Secure. Personnel files are confidential and are stored as such in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact *(Sharon Peach),* the Company's Data

Protection Officer. 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' consent to personal information being held

The Company holds personal data about its employees and, by signing your contract of employment, you have consented to that data about you being processed by the Company for any purpose related to your continuing employment or its termination including, but not limited to, payroll, human resources and business continuity planning purposes. Agreement to the Company processing your personal data is a condition of your employment. This includes giving your consent to the Company using your name, photograph and a brief work experience history in its marketing or promotional material, whether in hard copy print format or online on the Company's website. It also includes supplying the Company with any personal data that it may request from you from time to time as necessary for the performance of your contract of employment or the conduct of the Company's business, for example, supplying up-to-date contact telephone numbers to be held by line managers as part of its business continuity plan.

The Company also holds limited sensitive personal data about its employees and, by signing this policy, you give your explicit consent to our holding and processing that data, for example sickness absence records, particular health needs and equal opportunities monitoring data.

Employees' rights to access personal information

Under the Act, employees have the right to request to receive a copy of the personal data that the Company holds about them, including personal data held on personnel files that form part of a relevant filing system, and to demand that any inaccurate data held be corrected or removed.

Exemptions

There are a number of exemptions from the data protection regime set out in the Act, for example:

Confidential references that are given, but not those received by the Company from third parties. Only designated line managers can give Company references.
Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
Data which is required by law to be publicly available.
Documents subject to legal professional privilege.

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 line manager.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.

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.

Signed on behalf of the nursery	Print Name	Date